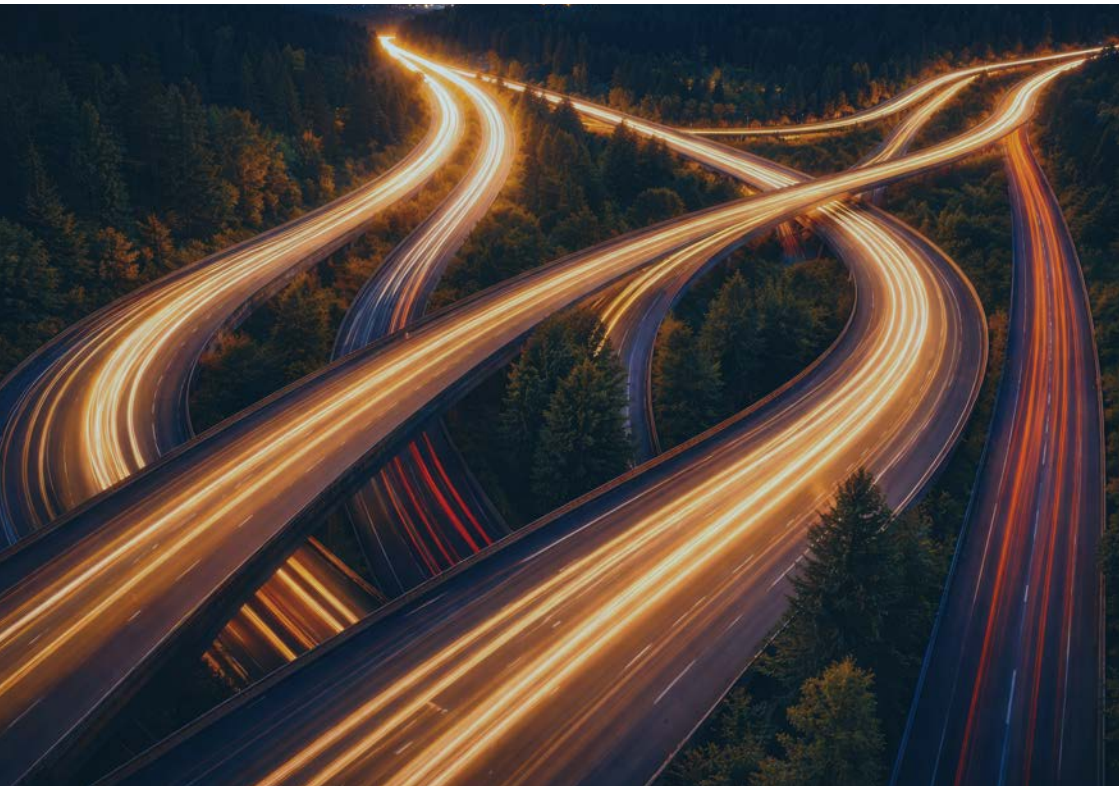
Why Websites Are Getting Hacked More Than Ever: What You Need To Do Now

Nicole Wallach
inMotion Real Estate Media



A prospect emails you Monday morning to say she got a strange follow-up after submitting a demo request through your site. The email used your company name and signed off with one of your salesperson's names. The wording felt off. The link in the email led to a phishing page. You check your contact form. It works. You check your CRM. The lead is there. Everything looks normal. You forward the email to your sales team and move on with your day.

Three weeks later, you find out that every form submission for the past two months has been copied straight to attackers, who've been running phishing campaigns against your prospects using details only your sales team should have had.

This story has gotten common in 2025 and 2026. The pattern is familiar to anyone working in website security right now, and it has very little to do with whether the site was built well or badly. The rules of the game have changed in the past 18 months, and most business owners haven't been told.

Two things are true at the same time, and both of them matter for anyone who owns a website.

First, the volume and nature of website attacks has shifted in a way that has no real precedent. AI tools have made attacking websites cheap, fast, and indiscriminate.

A single attacker working alone can now hit dozens of organizations a month. The economics of cybercrime have flipped: where attackers used to need skill, time, and money, they now need a chatbot subscription and an afternoon.

Second, your website is no longer a thing you build once and walk away from. It now needs the same kind of ongoing attention you give to any business-critical system: payroll software, accounting, your CRM. Things you check on, update, and watch for problems with.

This article walks through eight things you should know about the current threat environment as the owner of a US-based small or mid-sized business. By the end you'll understand why the volume of attacks has exploded, why your site is a target even if no one outside your customer base has heard of you, why the household-name companies getting hacked tell you almost nothing about the security of your own site, why you might already be hacked without knowing it, what your legal exposure actually looks like, why this is not about how your site was built, what cyber insurance covers (and what to ask any agency or vendor that touches your site), and what ongoing website protection should look like in 2026.

Some of what follows is uncomfortable reading. Most of what follows is fixable.

What actually changed

The shortest version of the story: attackers used to need skill, time, and money. Now they need a chatbot.

For most of the history of the web, hacking a website took real expertise. Whoever was going after your site had to know how to find vulnerabilities, write code that exploited them, set up the infrastructure to receive stolen data, and avoid getting caught. The pool of people with all four skills was small. The cost of going after any individual target was high. Small businesses mostly weren't worth the effort.

That's not where we are anymore.

AI tools now do most of the work that used to require a skilled attacker. Anthropic's August 2025 threat intelligence report documented a single individual using AI tools to run a data extortion operation against 17 organizations in a single month, including hospitals, government offices, emergency services, and religious institutions. A separate Anthropic report from November 2025 described state-linked attackers using AI to handle 80 to 90 percent of an attack campaign, including reconnaissance, vulnerability scanning, exploit generation, and data exfiltration, with humans only stepping in for high-level decisions. IBM published research showing that AI can produce a phishing campaign in five minutes that is nearly as effective as one a human expert would have spent 16 hours building.

Bots have also taken over the internet. Imperva's 2025 Bad Bot Report found that automated traffic reached 51% of all web traffic in 2024, surpassing human activity for the first time in a decade, with bad bots specifically accounting for 37% of all internet traffic: scanners, scrapers, credential

stuffers, and probe tools looking for openings. Cloudflare reports that bots make up 94% of all login attempts on its network. AI-enabled bot attacks went from 2 million per day to 25 million per day in a single year.

What this means in practical terms: if you put a website on the internet, automated systems will start probing it for weaknesses within minutes. The attackers don't choose your site. They sweep the entire internet looking for any site they can compromise.

And there's the speed at which new vulnerabilities get exploited. When a security flaw is discovered in WordPress, Shopify, or any of the underlying software your website depends on, the time between that flaw becoming public knowledge and attackers actively using it has collapsed. CyberMindr's analysis showed the average time-to-exploit dropped from 32 days in 2023 to 5 days in 2024. By 2025, security firm Hadrian's analysis of Mandiant data found exploitation was actually being observed before public disclosure in some cases. About half of all critical known vulnerabilities still hadn't been patched on most affected systems 55 days after a fix was available.

The reason this matters: even a perfectly built website becomes vulnerable the moment a flaw is discovered in any of its components. WordPress, the underlying software that runs about 43% of all websites globally, had nearly 8,000 new vulnerabilities disclosed in its plugin and theme ecosystem in 2024 alone, according to Patchstack's annual report. That's a 34% jump from the year before. Most of those flaws weren't in WordPress itself. They were in plugins: the add-ons that make WordPress sites do useful things like manage forms, run live chat, integrate with your CRM, and handle email automation.

Put these three things together and the picture is clear. The cost of attacking a website has collapsed, the volume of attacks has exploded, the attackers are using AI to do work that used to require teams of people, and they don't care who you are. They care whether they can get in.

Why your site is a target even if nobody's heard of you

The most common belief among small business owners about website security is that being small is a kind of protection. The thinking goes: hackers go after big companies with valuable data. We're a small operation, we don't handle any financial transactions through our site, we're not a household name. Why would anyone bother with us?

It's a reasonable belief. It used to be true. It is no longer true, and the reason is purely economic.

When attacking a website required skilled labor, attackers had to choose targets carefully. The expected payoff had to justify the time investment. Going after a 12-person consulting firm didn't make sense when you could spend the same effort on a Fortune 500 target.

Now that AI and automation handle most of the work, the cost of probing 10,000 websites is essentially the same as probing one. So they probe everything. The 80% of US small businesses that experienced at least one cyberattack in 2025, according to industry composite data, weren't picked. They were swept up.

The other piece most owners miss is what attackers actually do with a small business website once they get in. The valuable thing is rarely the data that lives on your site. It's what the site itself can be used for.

Here's a partial list of what a hacked B2B website is worth to attackers:

- Lead and prospect data, harvested from your contact forms, demo requests, content downloads, and quote requests. For a B2B company, this is often your most valuable digital asset: a list of named buyers at named companies, with declared pain points and budget signals. It gets sold to competitors, used for targeted phishing against those prospects, or both.

- Confidential business intelligence. B2B forms often capture pre-sales conversations: what the prospect is trying to solve, what they've already tried, what they're considering buying. Attackers who get into your form pipeline or CRM integration get a real-time view of your sales pipeline that competitors would pay for.

- Server resources, used for cryptocurrency mining or as a relay point for attacks on bigger targets. You pay the hosting bill. They get free compute.

- Sending platforms for spam and phishing. Your corporate domain has years of reputation built up. When attackers send phishing from your domain, it lands in your prospects' inboxes. By the time email providers notice and blacklist your domain, your sales team's email deliverability is destroyed for months.

- SEO injection. Attackers add hidden pages to your site that rank in Google for whatever they're selling: counterfeit goods, gambling sites, pirated software.

Your real pages keep working. Your visitors never see the spam. Google's crawlers do. Eventually Google penalizes your domain and your inbound organic lead pipeline collapses.

- Launching pad. Your site becomes the place from which attackers go after your customers and prospects. Phishing emails to your client list look legitimate because they come from you. Your customers get hit. Your customers blame you. Renewal conversations get harder.

Wordfence, which runs security for a large share of WordPress sites, blocked over 54 billion malicious requests against the sites it protects in 2024 alone. The company logged 8.7 million attacks against just two specific WordPress plugin vulnerabilities in a single 48-hour period in October 2025. Most of those attacks were against small business sites that had the affected plugins installed.

The takeaway: being unknown isn't a defense. The attackers don't know you and don't care. They scan, they get in where they can, and they take whatever value they can extract. Small sites often get probed harder than big ones because attackers correctly assume they have less defense in place.

Even Fortune 500 companies are getting hit

If size and security investment were enough to keep websites safe, the past two years should have been quiet for major corporations. They have not been.

In February 2024, Change Healthcare, a UnitedHealth Group subsidiary that processes about a third of all US medical claims, was breached by the BlackCat ransomware group. The attackers got in using stolen login credentials for a Citrix remote access portal that didn't have multi-factor authentication enabled. Once

inside, they encrypted critical systems and stole records belonging to roughly 190 million Americans, the largest healthcare data breach in US history. The attack froze pharmacy and claims systems across 94% of US hospitals. UnitedHealth ended up paying a $22 million ransom, then absorbed total costs of around $2.3 to $2.45 billion across 2024.

A multi-billion dollar healthcare conglomerate with a serious security budget was breached because one remote access portal didn't have MFA turned on.

In May 2025, Coinbase, the largest US-based cryptocurrency exchange, disclosed that overseas customer support contractors had been bribed to hand over customer data. There was no exotic technical exploit involved. People were paid money to give attackers access. The data was used in social engineering attacks against Coinbase customers, and the company disclosed in an SEC filing that it expects to pay between $180 million and $400 million in customer reimbursements and remediation.

In April and May 2025, the British retailers Marks & Spencer, Co-op, and Harrods were all hit by the same

ransomware operation, Scattered Spider, working with the DragonForce ransomware group. Marks & Spencer lost an estimated £300 million ($400 million) in profits and had online ordering down for over six weeks. Co-op had data on 6.5 million members stolen and lost £206 million ($277 million) in revenue. The attackers got in by calling third-party IT support staff and impersonating employees on the phone, convincing them to reset credentials. None of these companies had a "weak" website in any meaningful sense.

In September 2025, Jaguar Land Rover suffered what's been described as the most expensive security breach in British corporate history, with damages estimated at £1.9 billion ($2.5 billion). The Bank of England publicly noted the attack had measurably affected UK GDP growth.

These companies have hundreds or thousands of full-time security staff, seven and eight-figure security tooling budgets, dedicated incident response teams, and external auditors. They still got breached.

The point isn't that defense is hopeless. It isn't. The point is this: if Microsoft (which the company itself reports faces 600 million cyberattacks per day), UnitedHealth, Coinbase, and Marks & Spencer can all be breached in a 14-month period, the question for a small business owner isn't whether your website is built securely enough to repel attackers forever. The question is whether anyone is currently watching the site, ready to respond when something gets through.

The hack you don't notice

A persistent and dangerous belief in small business is that if your website got hacked, you'd know. Defacement, screens replaced with skull emojis, customer complaints flooding in, the site offline for days. You'd see it.

That's not how most attacks work in 2026. Most attacks are designed to stay hidden for as long as possible, because hidden means more time to extract value.

The economics here are simple. An attacker who breaks into your site and immediately defaces it gets a few hours of value before someone notices and shuts it down. An attacker who breaks in and stays unnoticed can spend weeks stealing prospect data, harvesting form submissions, building up SEO spam pages, mining crypto on your server, or hijacking your domain reputation. Hidden attacks pay much better. So that's what attackers do.

What does a hidden compromise actually look like? Here are some of the patterns happening right now:

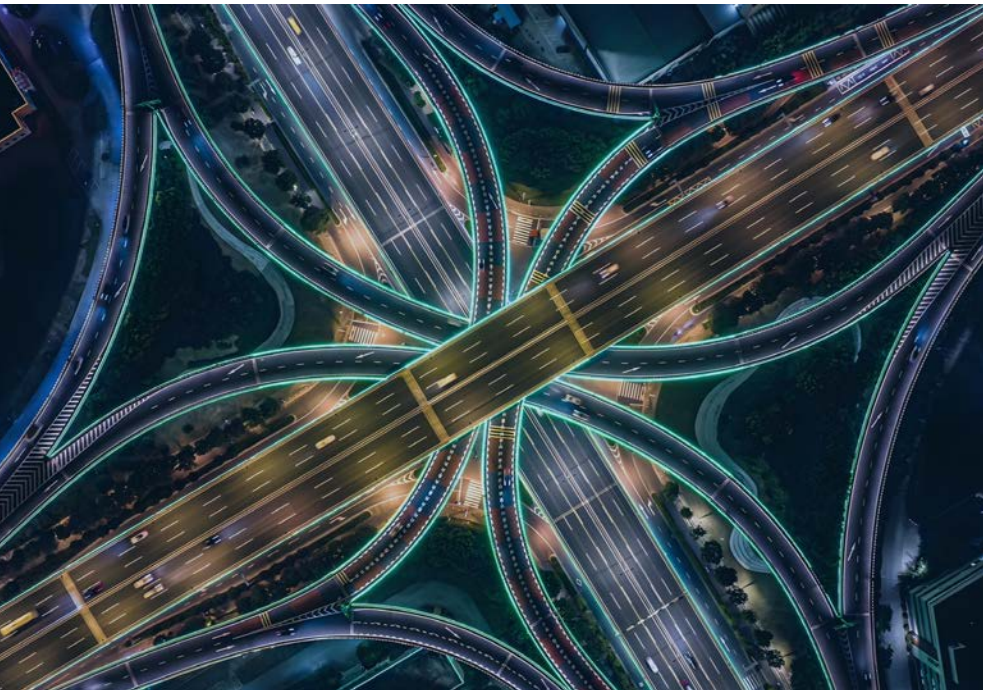
Form skimming. Attackers insert a few lines of JavaScript into your contact, demo, or quote forms. When a prospect fills in the form, the script copies the data to the attacker before the legitimate submission goes through. Your CRM still gets the lead. Your sales team sees nothing wrong. The attacker has every prospect's name, business email, company, phone number, and message in real time, alongside you. They can reach out to your prospect first, posing as you, before your sales team has even seen the lead arrive.

Conditional redirects. Attackers configure your site to behave one way for direct visitors (looks normal) and another way for visitors arriving from Google search (sent to a malicious site). You'll never see the redirect from your office. Prospects searching for you on Google will. Some will assume your business isn't legitimate and never come back.

Hidden admin accounts. Attackers create new administrator accounts on your CMS that don't appear in the standard user list, or that use names designed to look like system accounts. They have access. You don't see them. They can come back any time, including months after you've supposedly fixed the original problem.

SEO spam injection. Attackers add hundreds or thousands of pages to your site, hidden from your menus, that rank in Google for whatever they're selling: counterfeit goods, pharmaceuticals, gambling sites, pirated content. Your real pages keep working. Visitors browsing your site never see the spam. Google's crawlers do. Eventually Google notices, your domain reputation tanks, and your real pages stop ranking. By the time you call your marketing agency to ask why your inbound lead volume has dropped 60%, the damage has been baked in.

Form harvesting. Past form submissions stored on your site or in connected systems get pulled out in bulk. The attacker walks away with months or years of leads, sales conversations, and any documents that were uploaded through your forms. They sell the list. They use it for phishing campaigns against your prospects, with information only you should have had.



So how do you tell? Some signs to watch for, that you can ask whoever maintains your site to check on a regular basis:

- Unfamiliar admin or user accounts in your CMS
- Sudden drops in organic search traffic that aren't explained by anything you've changed
- Search Console warnings or notifications from Google about malware or hacked content
- Prospects or customers reporting that your site behaves oddly for them
- Unfamiliar pages indexed in Google when you search "site:yourcompany.com"
- Spikes in server resource usage that don't match your traffic
- Outgoing emails from your domain that you didn't send
- Unfamiliar files in your hosting account, particularly in plugin or theme directories

The key statistic here is dwell time: the average length of time between a system getting compromised and the compromise being detected. For SMBs without dedicated monitoring, this is often measured in months. Anthropic's August 2025 threat report described a state-linked AI-assisted campaign that ran for nine months across multiple targets before being identified.

If you don't have a system that's actively looking for these signs, you're effectively relying on someone outside your business: Google, a customer, your bank, a regulator, to tell you that you've been hacked. That's not a position any business owner wants to be in.

Your legal and financial exposure

This section is the one most likely to keep you up at night, so I'll be straightforward.

A hacked website is no longer just a technical problem with a technical fix. For a B2B company, it's a contractual, financial, and reputational event that can shake your customer relationships and your standing in your market. The exposure is serious enough to pose an existential threat to any small business that doesn't have a plan.

Start with the regulatory side. Every US state, plus DC and several territories, now has a data breach notification law on the books. For B2B sites that collect just business contact information through forms (name, business email, company, phone, role), state notification laws often don't directly trigger because that combination doesn't usually meet the legal threshold of "personal information." That's only true in the narrowest case, though. State laws do trigger if your site collects passwords for client portals, financial information, health information, or any combination of name plus a Social Security number, driver's license number, or payment card number. If your site has a client login area, a customer support form that collects identifying numbers, or anything that touches protected health information, you're squarely within the scope of state breach laws.

If you serve customers in California, the California Consumer Privacy Act (CCPA) and its expansion under the California Privacy Rights Act (CPRA) apply to most businesses doing significant volume there, including B2B. CCPA explicitly covers business-to-business contact data as personal information, and California residents have a private right of action over a breach. Class action attorneys watch breach notifications carefully.

Even where state breach notification laws don't trigger, regulators and private parties can still act. The Federal Trade Commission has pursued companies under Section 5 of the FTC Act for inadequate security practices regardless of company size or sector. State attorneys general bring parallel actions under their states' unfair-practices statutes. Affected individuals can also bring negligence claims directly, with no specific statute required.

The bigger exposure for most B2B businesses is somewhere else entirely:

- Customer contracts. Most B2B agreements above a certain size include security and breach notification clauses. If your customers learn about your breach from the news, you've broken a contract.

- Indemnification claims from customers. Most B2B contracts above a certain size include indemnification clauses that make you liable for losses your customers suffer when your breach cascades into their systems or data. A single such claim from an enterprise customer can dwarf the direct cost of the breach itself.

- Vendor risk reviews. Your customers' procurement and IT teams run periodic vendor reviews. A breach on file means questions, remediation demands, sometimes probation, sometimes removal from approved vendor lists.

- Compliance frameworks. If you market yourself as SOC 2 or ISO 27001 attested, an unhandled or unreported breach is an audit finding. Loss of attestation can be commercially fatal in some markets.

- Industry-specific regulation. If your customer base includes healthcare entities (HIPAA), financial services (GLBA), or federal government (FedRAMP, CMMC), the rules around your incident response are stricter and the penalties are higher.

- Confidentiality commitments. If your site holds gated content, partner-shared documents, pricing sheets, or proposal templates, exposing them breaks the commitments you made to whoever provided that material.

On top of all that, there are the direct costs of incident response. The IBM Cost of a Data Breach 2025 report put the global average at $4.44 million, though that figure includes large enterprise incidents. For genuine small businesses, TechAisle's 2025 data put the average breach cost at around $1.6 million. Microsoft's 2024 reporting on companies in the 25 to 299 employee range showed an average of about $254,000 per incident, with some incidents running up to $7 million.

What goes into those numbers:

- Forensic investigation, to figure out what happened and what data was taken (typically $25,000 to $250,000 for SMBs)

- Notification costs, including written notices, postage, call center support, and credit monitoring services

- Legal fees defending against private lawsuits and regulatory actions

- Regulatory fines, where applicable

- Settlement costs for class actions

- Customer compensation

- Lost business while systems are down or while you're rebuilding trust

- Increased insurance premiums afterward

A major breach poses an existential financial threat to any small business that doesn't have reserves, insurance, and a response plan in place.

Beyond the direct costs, the relationship damage in B2B is often the bigger number. A single breach can cost you a flagship enterprise account whose lifetime value dwarfs the direct cost of incident response.

A breach is no longer a technical incident with a technical recovery. It's a business event with a long tail of legal, financial, and relational consequences.

This isn't about how your site was built

If you've read this far, you might reasonably be wondering: if my website is at this much risk, did the people who built it do something wrong?

The honest answer is no. Website security has two phases, and they have to be understood separately.

The first phase is the build. This is what your agency delivers when your site goes live. It includes the architecture and platform choices, the secure coding practices used to develop custom features, the configuration of the servers and CMS, the vetting of plugins and third-party tools, the setup of access controls and authentication, and the initial hardening against the threats known at the time of launch. A well-built site starts with a foundation that's appropriate for the threats that exist when it's deployed. This is what inMotion Real Estate delivers and stands behind.

The second phase is the operating environment. This is everything that happens after the site goes live, for as long as the site exists. It includes the patches that get released as new vulnerabilities are discovered (in WordPress core, in your plugins, in your hosting infrastructure, in the underlying operating system); the monitoring that detects

when something starts going wrong; the response when something does go wrong; and the regular reviews that catch issues before they become incidents.

Imagine you have a building inspector certify your house when it's built. They check the wiring, the plumbing, the structure. They sign off. The house is built well. None of that means the locks on the door never need to be changed, the smoke detector batteries never need to be replaced, the alarm system doesn't need monitoring, or the neighborhood will never have a crime wave. The certification was about the build. The ongoing safety of the home is a different category of work, and it never ends.

Website security works the same way. A site built well in 2023 was secure against the threats of 2023. The threats of 2026 are different in scale, character, and speed. No amount of build-time work, however careful, can address attacks that hadn't been invented when the build happened.

The need for ongoing security work is not a comment on the original build. It's a fact of operating a website on the modern internet.

Cyber insurance and what to ask any vendor

Cyber insurance has become as important to a small business as general liability insurance. If you don't have it, the costs in the previous section come out of your operating capital. If you do have it, most of those costs are covered, and you have a hotline to call when something happens.

What cyber insurance typically covers, in plain terms:

- Breach response costs: forensic investigation, notification, credit monitoring, customer call centers
- Legal fees for regulatory defense and civil claims
- Public relations support
- Business interruption losses while your systems are offline
- Data recovery and system restoration costs
- Cyber extortion payments (where the policy allows them)
- Some third-party liability coverage when your incident affects customers or partners

What it typically doesn't cover: loss of intellectual property, reputational harm beyond a defined window, fines that aren't legally insurable in your state, and incidents arising from negligence the policy excludes (such as failing to apply patches the policy requires you to apply).

Now the part that catches most business owners off guard. If your agency has access to your website, your CMS, your hosting account, your customer database, or any of your credentials, then your agency is part of your attack surface. If your agency gets compromised, your

site can be compromised through them. If your agency is uninsured, the costs of that compromise come from somewhere, and that somewhere is most often you.

This is why asking the right questions of any vendor or agency that touches your website matters. Some questions worth asking, regardless of who you're working with:

- Does your firm carry cyber liability insurance? Through what carrier?
- What's the policy limit? (For a working agency, $1 million is a reasonable minimum, $2 million is more common, larger firms carry $5 million or more.)
- Does the policy cover incidents originating in your systems that affect our website or our customer data?
- What's your incident response process if our site is compromised? Who do we call, what's the time-to-response, what do you do in the first 24 hours?
- How do you store our credentials, and who has access to them?
- Do you have written security policies your team follows, and can we see them?
- When was your last third-party security review or audit?
- What happens to our access and data if we end the relationship?

These aren't gotcha questions. They're questions that any vendor handling business-critical infrastructure should be able to answer in writing within a few business days. If a vendor can't answer them, or doesn't have insurance, that's information you need to make a decision about the relationship.

For our part: inMotion Real Estate carries cyber liability insurance through a top-rated US carrier, and we're happy

to share our certificate of insurance with any client who asks. The reason this is set up the way it is: if something happens that traces back to us, our clients aren't left to absorb the consequences alone. That's table stakes for any agency operating in 2026, in our view.

If you work with multiple vendors who touch your website, run these questions past all of them. Common gaps we see in client environments include hosting providers without coverage adequate for their role, design or development contractors with no policy at all, and IT firms whose general liability coverage doesn't extend to cyber events. Every gap in coverage is potential exposure for you.

What ongoing protection actually looks like

Everything in this article points to one conclusion: a website in 2026 needs ongoing attention from someone who knows what to look for. That attention has four basic components.

Start with software updates and patching. Every component of a modern website (the CMS, the plugins, the theme, the libraries those plugins depend on, the

server software, the underlying operating system) gets updates regularly, and many of those updates fix newly discovered security flaws. Patching used to be something done quarterly. The data covered earlier in this article shows why that no longer works: vulnerabilities are being exploited within days or even before public disclosure now. Patching is a continuous process. For a typical small business website running on WordPress, that means updates being reviewed and applied on a weekly or near-weekly basis, with critical patches applied within hours of release. This work needs to happen. The question is who does it.

Monitoring matters too. Something or someone has to be watching for the signs covered earlier in this article. This includes file integrity monitoring (alerting when files on your site change unexpectedly), traffic monitoring (alerting on unusual patterns), uptime monitoring, search console monitoring, and periodic manual review. Tools handle most of this work, but tools alone don't replace someone who can interpret the alerts and decide what's a real problem versus a false alarm.

Backups and recovery come next. Backups need to be recent, tested, and stored away from the live site. Recent because anything older than a day means losing transactions and data. Tested because untested backups have a habit of failing when you need them. Stored away from the live site because attackers who get into your hosting account often delete or encrypt backups stored there as part of the attack. A workable backup setup typically involves daily automated backups with a defined retention period, stored in a separate cloud account with separate credentials, and a documented restoration process that's been actually tried at least once.

Last is incident response. When something is detected (and statistically, eventually something will be detected), there has to be a plan. Who gets called. What gets shut down. Who handles communications with affected customers, regulators, and your insurer. Who handles forensic investigation. Who handles the rebuild. The middle of an active incident is the worst time to figure out the answers to those questions.

For most SMBs, doing all four of these in-house isn't realistic. It requires either dedicated security staff or someone with the time, expertise, and tools to handle it as part of a broader role, and most small businesses don't have either. The practical options are: hire a specialized website security firm (typically $200 to $1,500 per month depending on scope and site complexity), bring it into your IT services contract if you have one, or include it in an ongoing maintenance arrangement with the agency that built and understands your site.

The wrong answer is to do none of it.

Closing

Websites used to be assets you built and forgot about. They aren't anymore. The data above tells a clear story: attack volumes are at record levels, AI has dropped the cost of attacks to near zero, and even organizations with massive security budgets are getting breached regularly. Small businesses are being hit harder than any other category, and the legal and financial exposure when something goes wrong has gotten serious.

Your website may have been built well. Modern threats outpace anything that build-time work alone can address, which is why ongoing protection has to be part of how you think about the site going forward.

The good news: ongoing protection is achievable, affordable, and well within reach for any business that decides to take it seriously. The hard part is the deciding.

If you're an inMotion Real Estate client and you aren't sure what level of monitoring and maintenance you currently have in place, the next step is a 20-minute call with our team. We'll walk through what's covered today, what isn't, what the gaps look like for your specific site, and what a sensible level of ongoing protection would cost. Whether the right answer is working with us or working with someone else, the goal is to make sure someone is watching your site.

inMotion Real Estate Media is a commercial real estate marketing and design agency serving CRE firms across North America. Founded in 2006 and operating as part of the Hudson Fusion group, inMotion has completed more than 200 client engagements, working with major industry names including JLL, Cushman & Wakefield, CBRE, Newmark, Avison Young, and Marcus & Millichap. The agency focuses exclusively on commercial real estate, offering custom web development, digital marketing, technology and CRM integrations, graphic design, investor outreach through its Investor Connect service, and a Visibility service line for CRE firms. With nearly two decades of category specialization, inMotion builds award-winning websites and marketing campaigns for CRE companies and the properties in their portfolios.