

Data Privacy, Security, Safety & Risk Management

September 30, 2026

Billions at Risk: Hundreds of New Domain Extensions Are Coming. Is Your Company Ready?

By [Amy S. Mushahwar](#)

Executive Summary

Weak domain security contributes to some of the most expensive cyber losses. A payment wire that goes to the wrong account. A mailbox that an attacker has had access to for weeks. An outage that takes a customer portal down for two days. The resulting claims may be classified as funds transfer fraud, business email compromise, or business interruption. But in a meaningful share of these incidents, the underlying weakness is the company's domain.

Most companies treat their internet domain as an address. In practice, a company's primary domain carries its email, employee logins, website certificates, and the links customers are taught to trust. Whoever controls the domain can control much of what depends on it. That is what makes the domain a root of trust.¹

Two developments make this timely. Artificial intelligence (AI) has reduced the time, cost, and skill required to impersonate a company. ICANN, the nonprofit that coordinates the internet's naming system², is also preparing to add hundreds of new domain extensions, giving impersonators more places to operate. AI does not create the underlying domain weakness. It makes that weakness easier to discover, exploit, and scale. Insureds and insurers should treat domain security as a core control, on the same footing as multifactor authentication (MFA), endpoint protection, and backups.

ICANN has confirmed that 1,616 applications for new generic top-level domains³ will proceed in its 2026 round. On September 29, ICANN confirmed that [Reveal Day will take place on October 7, 2026](#), when it will publish the applied-for strings, any variant or replacement strings, and the contention sets identifying which extensions drew competing applicants. Applicants then have 14 days to switch to a pre-designated replacement string before String Confirmation Day fixes the field. This is the program's second round, 14 years after the first. Commentators have already noted that the expansion will open new space for infringement and abuse and that brand owners should prepare.

I spent the first decade of my career working on domain security. The question then was mostly about trademarks. The question now is about loss.

Why the Domain Is a Root of Trust:

Domain security matters because the primary domain anchors corporate email, single sign-on authentication, password-reset messages, website certificates,⁴ vendor payment instructions, and the links customers are trained to trust. Whoever controls a company's DNS can, in many configurations, redirect its email, obtain valid certificates in its name, and intercept the messages that let someone reset a password. The registrar account and the DNS settings together are a master key, and that key often sits outside the security program's line of sight. Two companies typically stand behind a domain registration. The registrar sells the name and holds the account

that an administrator logs in to manage it. The registry operates the extension itself.⁵ The distinction matters, because a lock applied at the registry level is designed to hold even after a registrar account has been compromised.

The attacks are rarely exotic. A registrar account protected by a single password gets phished. A forgotten domain lapses and is re-registered by a stranger, who then begins receiving password-reset emails for every service still tied to it. A subdomain points to a cloud service the company no longer uses, and someone else claims it.⁶ A lookalike domain, one character off from the real one, sends wire instructions to a customer.⁷

Why Does Domain Risk Fall Through the Cracks?

Responsibility is split. In many organizations the registrar account belongs to marketing or IT operations, trademark enforcement belongs to legal, and email authentication belongs to the security team. Each group sees one piece, so even experienced security professionals may lack a full view of how domains fail. It is common to find a mature program that has locked down laptops, servers, and logins while the registrar account that controls the company's DNS sits outside the company's central login system, protected by a shared password and a personal mobile number. The policy and contractual layer is also unfamiliar to most technical teams: how registrars handle transfers, how disputes and takedowns move through ICANN's procedures or under federal law,⁸ and what a registry will or will not do in an emergency. Much of the practical ability to fix a problem sits in that layer.

Part of the reason the problem persists is economic. The domain business runs on per-registration fees, and a registration generally earns the registry and the registrar the same fee whether the buyer is a brand owner, a speculator, or a fraudster. Typosquatted and lookalike domains represent volume, and volume represents revenue for the parties selling the names, even when no one intends that result. Brand owners feel the pressure from the other direction: defensive registrations, premium pricing on brand-adjacent names, and blocking products⁹ add up to a recurring cost for companies simply trying to keep their names out of the wrong hands. Parked lookalike domains¹⁰ may also earn money from advertising and traffic resales.

Many registries, registrars, and privacy providers spend real money on abuse mitigation. The problem is structural: the commercial incentives do not naturally align with an insured's interest in fewer lookalike domains and faster takedowns. That gap is why insureds should take an active role in their own domain security and why the controls discussed below matter.

How AI and New Extensions Expand the Exposure

For most insureds, the exposure sits in the registrar and the DNS accounts they already have, the domains they have forgotten they own, and the lookalike domains others register to impersonate them. More extensions will likely mean more places for those lookalikes to live. Brand owners will still want to confirm that their marks are recorded in ICANN's Trademark Clearinghouse before the new extensions launch, because that record is what gives them early access to matching names and notice when someone else registers one.

Domain portfolios accumulate through acquisitions, marketing campaigns, product launches, rebrands, foreign subsidiaries, and one-off registrations made to get a project moving. They often end up spread across several registrars, with inconsistent renewal settings, stale DNS records, and account owners who have left the company. When domain security is weak, the resulting loss appears on the claim as a fraudulent transfer, a compromised mailbox, or an outage. Few claims are ever labeled a domain event.

Six Controls That Matter

Monitoring matters, but it reports a problem only after someone else has created it. Six preventive controls do more of the work.

1. **Inventory domains, consolidate them to one account and harden it.** Once you inventory the portfolio, move it to a corporate registrar,¹¹ limit access to a small number of named administrators, and protect those accounts with phishing-resistant MFA.¹²
2. **Registry lock on the domains used for email and logins.**¹³ The registry will then refuse to process a transfer or a change to the DNS settings until it has verified the request with named contacts through a separate channel, so a compromised registrar login alone should not be enough to move the domain.
3. **Renewal governance.** Enable auto-renew, assign a named owner, and require a deliberate decision before any domain is allowed to lapse.
4. **Email authentication.** The SPF, DKIM, and DMARC standards let a company tell the world's mail systems which servers may send email in its name and what to do with messages that fail the check.¹⁴ The setting that matters is enforcement; a DMARC record left in monitoring mode reports spoofing without stopping it. Domains that never send mail should be locked down too, so they cannot be spoofed.
5. **DNS hygiene.** Restrict which certificate authorities may issue certificates for the domain, watch for certificates issued without authorization,¹⁵ and periodically remove DNS entries that point to services the company no longer uses.
6. **A written takedown and escalation playbook.** Keep registrar contacts and a pre-arranged takedown vendor in the incident response plan, so no one is searching for a login in the middle of an event.

What Clients and Counsel Should Ask

Domain security also has a contractual side that lawyers should consider when advising clients. Registrar and DNS provider agreements vary widely. Four provisions deserve the most attention.

1. **Service levels for incident response.** How quickly will the provider act on an urgent request to lock a domain, reverse an unauthorized transfer, or restore a hijacked one? Some corporate registrars offer 24/7 support and committed response times; others do not. A named security escalation path and a committed response time for lock and transfer-reversal requests are reasonable asks.
2. **Liability and indemnification.** Many registrar agreements contain broad limitations of liability and require the registrant to indemnify the registrar for claims arising from the domain's use. These provisions may limit recourse if the registrar's own security failure contributes to a loss. A carve-out from the liability cap for the provider's own security failures is worth raising, and corporate registrars may be more receptive to it than retail providers.
3. **Dispute resolution and governing law.** These clauses affect where and how a registrant pursues remedies, which matters when speed is critical. A registrant that may need emergency relief will want a forum where a temporary restraining order is realistic and a provider that commits to act on court orders promptly.
4. **Data retention and cooperation.** These provisions determine whether the provider will preserve evidence and cooperate with investigations or litigation. A stated retention period for account and DNS change logs, and a commitment to preserve records on request, can decide whether a loss can be attributed to anyone at all.

Insureds with significant domain portfolios should review these terms as part of vendor due diligence.

How AI Complicates and Improves Domain Security

On the threat side, AI lowers the cost of impersonation. Generating hundreds of lookalike domains, cloning a website convincingly, and writing well-crafted phishing lures in any language now takes minutes. Pairing a lookalike domain with a synthetic (deepfake) voice or video of an executive makes payment fraud more

persuasive. AI agents that browse, click, and transact on a user's behalf raise a further concern, because they may act on a domain name with less skepticism than a trained employee would.

On the defense side, AI is useful. It can classify newly registered domains at scale, detect visual and phonetic similarity to a brand, triage monitoring alerts that would otherwise overwhelm a small team, and help reconcile messy inventories across registrars and DNS providers. Organizations that automate discovery and response will keep pace more easily than those that rely on manual review as attack volume grows.

How Carrier Tools Can Help Insureds Get Organized

The application process is an underused lever. Many carriers already run external scans that surface email authentication gaps, exposed services, and certificate problems. Adding domain-specific questions—how many domains the applicant holds, which registrars hold them, whether registry lock is in place, and who owns renewals—often forces the insured to find out. For many organizations, the application is the first time anyone has tried to assemble the inventory.

Carriers can amplify that effect by sharing scan results with the applicant instead of using them only for pricing and by pointing insureds toward remediation resources before bind.

Domain Risk in Underwriting

A reasonable starting point is to treat domain security as one of the controls the underwriter evaluates, alongside MFA, endpoint protection, and backups. Underwriters might ask whether the portfolio is consolidated, whether critical domains are locked, whether email authentication is set to enforcement, whether there is a named owner and a renewal process, and how the domains of acquired companies were absorbed. Acquired companies are the most common blind spot. Portfolios also accumulate informally, through marketing campaigns, product launches, rebrands, and foreign subsidiaries, among other reasons. An applicant who cannot produce a reconciled inventory showing every domain, who controls it, when it renews, and what depends on it has answered the question.

Two further points deserve attention. First, domain risk changes continuously, so point-in-time answers age quickly; periodic or continuous scanning during the policy period may give a truer picture. Second, concentration among a small number of registrars and DNS providers raises aggregation questions, since an incident at a widely used provider could affect many insureds at once. As the new extensions from the 2026 round go live, carriers may also want to watch whether impersonation activity shifts into them.

Are Goodwill Losses Covered?

Coverage depends on the wording and the facts. A domain event can damage customer trust, interrupt operations, divert traffic, and enable payment fraud. Cyber policies may respond through crisis management, business interruption, reputational harm, funds transfer fraud, or social engineering coverage, often subject to sublimits and verification conditions. Many forms, however, limit or exclude future revenue, diminished brand value, and similar intangible harms. Insureds concerned about brand-level loss should review how the policy defines covered loss and how it treats lookalike-domain fraud when customers are the direct victims.

Value-Added Services and Premium Credits

Value-added services make sense, because domain controls are inexpensive and many insureds have simply never thought about them. Carriers and brokers could offer pre-bind domain scans with the findings shared back, panel vendors for monitoring and takedown, help setting up DMARC, and guidance on registry lock.

Premium credits are more complicated. They depend on rating plans, regulatory filings, and whether the carrier can verify the control over time. Where that is feasible, tying a credit to a verifiable control, such as registry lock or DMARC enforcement, may mean more than tying it to an answer on the application.

One Control I Recommend

If an insured does one thing, I suggest placing registry lock on the domains used for its email and logins, held at a corporate registrar with phishing-resistant MFA and a short list of named administrators. It addresses the scenario with the broadest consequences—the silent takeover of the domain that everything else depends on. Because the lock is held at the registry, above the registrar account most likely to be phished, it holds even when that account is compromised. It is also modest in cost relative to the exposure. DMARC enforcement would be a close second.

Looking Ahead

With Reveal Day set for October 7, hundreds of new extensions are on the way, and impersonators will have more room to work. I will be moderating the “Billions at Risk: AI, Domains & Cyber Loss” panel at the NetDiligence Cyber Risk Summit in Philadelphia on October 6; details are at <https://www.lowenstein.com/news-insights/events/billions-at-risk-ai-domains-cyber-loss-mushahwar>.

The companies that fare best will likely be the ones that know what they own, understand what depends on it, and lock their critical domains. They will be better positioned to prevent the next domain event, and to prove what happened when prevention fails.

¹ In security engineering, a trust root (or root of trust) is the component that everything else relies on to verify identity. If it is compromised, the systems built on it can no longer tell a legitimate request from a forged one. A company's primary domain plays this role for its email, its logins, and its website.

² The Internet Corporation for Assigned Names and Numbers (ICANN) sets the rules for the Domain Name System (DNS), which translates names like example.com into numeric addresses. ICANN accredits the registrars that sell domains and contracts with the registries that operate each extension.

³ A generic top-level domain (gTLD) is the part of a web address after the final dot, such as .com or .org. ICANN's 2026 round lets companies and other organizations apply to operate new extensions, including a .brand of their own. Applications remain confidential until Reveal Day.

⁴ A Transport Layer Security certificate is the credential that lets a browser confirm it is talking to the real owner of a website. Certificate authorities issue them to whoever can prove control of the domain, so an attacker that controls the DNS can obtain a valid certificate and run a convincing fake site that raises no browser warning.

⁵ For .com, for example, the registry is Verisign; retail and corporate registrars sell .com names to the public and manage them on the registrant's behalf. ICANN accredits registrars and contracts with registries, and its policies govern transfers, expirations, and disputes.

⁶ This is known as subdomain takeover. Companies often point a subdomain, such as promo.example.com, at a cloud host or marketing platform. If the service is canceled but the DNS entry remains, anyone who signs up for the same service can claim the name and publish content, or collect email, under the company's brand.

⁷ A lookalike domain is one designed to be mistaken for a legitimate one, whether through a misspelling (typosquatting), a swapped character, a different extension, or an added word. Attackers use lookalikes to send email that appears to come from the company and to host copies of its website.

⁸ Two ICANN procedures apply to nearly all generic domains. The Uniform Domain-Name Dispute-Resolution Policy can transfer or cancel a domain registered in bad faith. The Uniform Rapid Suspension is a faster alternative for clear-cut cases but can only suspend a domain. In the United States, the Anticybersquatting Consumer Protection Act provides a federal cause of action for bad faith registration of a confusingly similar domain.

⁹ A blocking product is a service, sold by registries or through them, that prevents anyone from registering a given brand name across many extensions at once for a single fee, as an alternative to registering the name defensively in each extension.

¹⁰ A parked domain is registered but not used for a working website or email. It typically displays advertising links, and the holder earns a share of the revenue when visitors click on them, including visitors who arrived by mistyping a brand name.

¹¹ A corporate (or enterprise) registrar is built for business customers. It typically offers dedicated account teams, stronger login controls, support for registry lock, and consolidated billing across a large portfolio. Retail registrars are built for volume and price, and their account security reflects that.

¹² MFA requires a second proof of identity beyond a password. Phishing-resistant MFA uses a hardware security key or passkey cryptographically tied to the genuine website so it cannot be replayed on a fake login page.

¹³ Registry lock is a service offered by most major registries through participating registrars. While the lock is in place, the registry will not process changes to the domain's ownership, registrar, or DNS settings until the request has been confirmed with preauthorized contacts by an agreed-upon method, typically a phone call asking for a passphrase. Pricing varies by registrar but is typically a few hundred dollars per domain per year.

¹⁴ SPF (Sender Policy Framework) lists the servers allowed to send email for a domain. DKIM (DomainKeys Identified Mail) adds a digital signature to outgoing messages so that recipients can verify they were not altered. DMARC (Domain-based Message Authentication, Reporting and Conformance) tells receiving mail systems what to do when a message fails those checks and sends the domain owner reports. A DMARC policy of "none" only monitors, "quarantine" sends failing mail to spam, and "reject" blocks it. Only the last two count as enforcement.

¹⁵ A Certification Authority Authorization record is a DNS entry that lists the certificate authorities permitted to issue certificates for a domain. Certificate transparency logs are public records of every certificate issued by the major authorities; monitoring them alerts a company when a certificate for its domain has been issued to someone else.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR

Partner

Chair, Data Privacy, Security, Safety & Risk Management

T: 202.753.3825

amushahwar@lowenstein.com

NEW YORK

PALO ALTO

ROSELAND

SALT LAKE CITY

SAN FRANCISCO

WASHINGTON, D.C.

WILMINGTON

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.