



The ROI of DNS:

A Guide to Risk Reduction and Smart Investment



Making the business case for DNS security: costs, risk mitigation, and ROI

For large enterprises, securing domain name system (DNS) infrastructure is a business imperative. DNS failures can result in significant downtime, legal exposure, and reputation damage. However, domain security is often overlooked in broader cybersecurity strategies.

This insight paper helps decision-makers build a compelling business case for DNS security by outlining the costs of failure and practical ways to communicate risk and return on investment (ROI).

The true cost of failing DNS security

A DNS security failure can trigger a cascade of consequences far beyond initial downtime. While lost revenue during an outage is often the most visible cost, indirect impacts such as compliance concerns, legal costs, and reputation damage can be harder to quantify and may be more expensive over time.

Cybersecurity leaders increasingly view domain-based threats as material business risks, not isolated technical issues. In CISO Outlook 2025, 70% of respondents expect security threats to increase, and 98% predict an increase over the next three years.¹ As the threat landscape intensifies, organizations need to prioritize foundational controls that support uptime, customer trust, and business continuity.

“I’ve seen teams work around the clock to recover from a DNS disruption, only to be asked afterward why the business didn’t have stronger protections in place. That’s why it’s important to treat DNS security as a planned investment, not an after-the-fact fix.”

Mark Flegg

Senior Director, Security Products and Services, CSC

Direct vs. indirect costs: a growing ripple effect

Direct costs are immediate and measurable expenses when critical services go offline, such as:



Downtime losses—
Disrupted operations,
transaction failures, and
customer churn

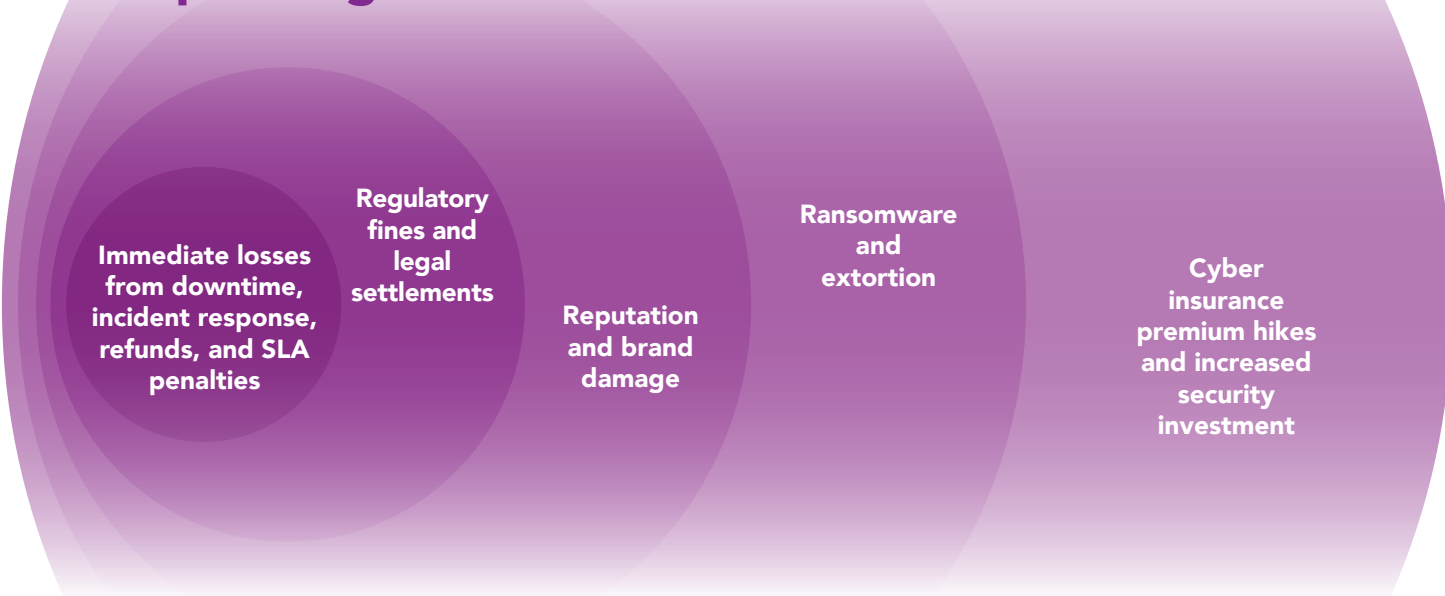


**Emergency IT support
and incident response**—
Internal IT teams or
external specialists working
to diagnose and restore
services



**Refunds and service
level agreement (SLA)
penalties**—Compensation
owed to customers or
partners due to SLA
breaches

The expanding wave of hidden costs



However, direct costs are only the first wave of financial impact, as revealed by a Splunk report.² As the ripple effect spreads outward, the indirect costs hidden beneath the surface begin to accumulate, capable of eclipsing the initial expenses.



Regulatory fines and legal settlements—Enterprises operating in regulated industries may face compliance violations and lawsuits due to service disruptions or data breaches.



Reputation and brand damage—Lost customer trust can have long-term effects on market position, customer retention, and revenue growth. Organizations may also need to reassure stakeholders, address concerns from investors, and provide transparency about incident response efforts.



Ransomware or extortion demands—If attackers manipulate DNS settings to redirect traffic or block access, businesses may face financial extortion attempts.



Higher cyber insurance premiums and increased security investment—A DNS failure, particularly one involving a security breach, can lead to higher insurance costs as insurers assess increased risk exposure.

Aiming for “five nines” uptime, but asking smarter questions

For enterprises, uptime expectations are high. The “five nines” principle, or 99.999% uptime, translates to less than five minutes of downtime per year. Many organizations treat this as a benchmark for reliability, but DNS service commitments vary by provider and service tier. In practice, a provider’s real-world track record, especially under stress or attack, is often a better indicator than theoretical uptime targets.

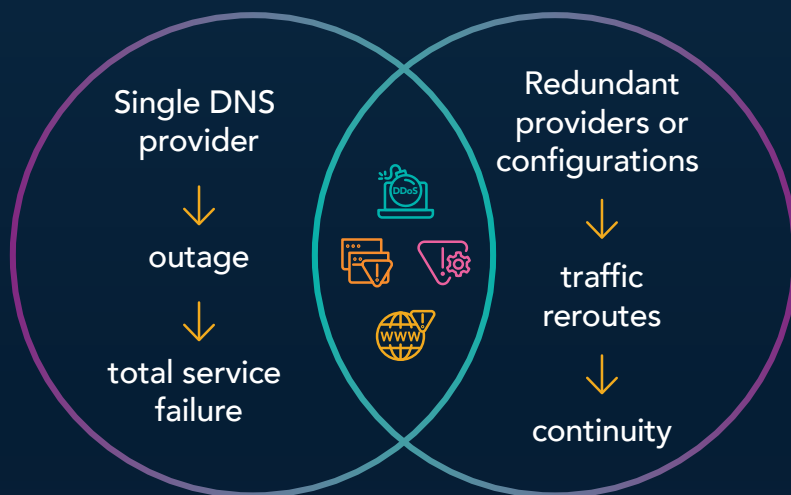
Many enterprises now rely on cloud-based infrastructure and third-party platforms to support customer-facing services, internal applications, and business-critical workflows. While these providers can improve scalability and performance, they can also introduce risk to operations, especially when availability depends on one single provider, region, or configuration. DNS resilience planning should include redundancy strategies designed to maintain availability during outages, misconfigurations, or upstream degradation.

“Enterprises plan for failure everywhere else—multiple regions, backups, failover systems. But too often, DNS is still treated as ‘good enough’ with a single provider or configuration. That’s a risky assumption for something every digital service depends on.”

Mark Flegg
Senior Director, Security Products and Services, CSC

Single-point DNS risk vs. resilient DNS architecture

Together, these risks show why DNS security should be treated as a core part of enterprise risk reduction, not a secondary IT consideration. Furthermore, the CISO Outlook 2025 found that chief information security officers (CISOs) ranked domain and DNS hijacking among the top expected threats over the next three years.³



DNS plays a foundational role in keeping websites, email, and internal applications available, yet it’s often under-protected. The risks are significant and include:

Distributed Denial-of-Service (DDoS) attacks: Malicious actors target DNS infrastructure with high-volume attacks, overwhelming servers and causing outages.

Provider outages: Enterprises relying on a single DNS provider risk complete failure if that provider experiences downtime.

Configuration errors: Simple misconfigurations, such as improper DNS record changes, can disrupt entire services.

Domain hijacking: Unauthorized changes at the registrar level can redirect traffic, leading to reputation and security risks.

Quantifying the cost of a DNS failure

For enterprises looking to assess and communicate the financial impact of DNS security risks, the annualized loss expectancy (ALE) formula provides a structured approach to quantifying potential losses. This methodology helps cybersecurity leaders translate technical risks into business-focused financial terms, making it easier to justify proactive investments in DNS security.

The ALE formula is defined as:

$$\text{SLE} \times \text{ARO} = \text{ALE}$$

Single loss expectancy (SLE): The financial impact of a single DNS failure, including direct (and, if possible, indirect) costs.

Annual rate of occurrence (ARO): The estimated number of times such an incident is expected to happen in a year.

Annualized loss expectancy (ALE): The projected yearly financial loss due to DNS security failures.

By calculating SLE and ARO based on an organization's risk landscape, enterprises can create an ALE figure—a concrete way to measure potential financial exposure and justify preventative investments in DNS security.

“Many organizations struggle to quantify the cost of DNS-related threats, making security investments harder to justify. The ALE formula provides a practical model for financial risk, helping decision-makers see the business impact of proactive DNS security.”

Mark Eggleston
CISO, CSC

Communicating the business value of DNS security

Despite growing awareness of domain-based threats, many organizations still feel underprepared. In CISO Outlook 2025, only 22% of respondents said they have the right tools in place to counter domain-based threats.⁴ This gap between risk and readiness is exactly where ROI-focused DNS initiatives can make the strongest case.

To secure funding, cybersecurity leaders must translate DNS risk into business impact by connecting domain security to uptime, customer trust, compliance exposure, and operations resilience.

“DNS wasn’t designed for today’s threat landscape, but it’s still the system we rely on to route customers, employees, and partners to the right place. That’s why DNS security deserves the same level of attention as other core controls.

Mark Flegg

Senior Director, Security Products and Services, CSC

Understanding your audience: tailoring the message

To secure DNS security investment, cybersecurity leaders must align their messaging with the priorities of different stakeholders. Security teams may focus on technical risks, while other departments have other business objectives, financial concerns, and operations challenges. Positioning DNS security in relation to each team’s self-interest increases the likelihood of gaining their support.





Executives: the business impact of DNS security

Senior leadership is focused on financial performance, risk management, and competitive positioning. Because DNS is essential to uptime, it's also core to business continuity and disaster recovery—two top priorities for senior leaders. Framing DNS as a strategic investment, not just an IT expense, helps connect it to broader organizational resilience.



Board members aren't focused on DNS—they care about brand protection and cybersecurity risks. Avoid technical details and frame the discussion in business terms. For a primer, read up on how cybersecurity is discussed in publications such as The Wall Street Journal.

Mark Eggleston
CISO, CSC



Legal teams: regulatory compliance and liability reduction

Corporate legal teams prioritize compliance with industry regulations and reducing liability exposure. Many data privacy and security frameworks, including the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Network and Information Security Directive (NIS2), require strong security controls to protect sensitive information. Without proper DNS security, companies risk data breaches, phishing incidents, and unauthorized domain transfers, all of which can lead to legal action or penalties.



Marketing and brand teams: reputation protection and phishing prevention

Marketing teams are responsible for brand reputation, customer trust, and digital engagement, all of which can be compromised by DNS-related threats. Positioning DNS security as a brand protection strategy rather than just an IT concern makes it more relevant to this audience.



Domain security extends beyond traditional cybersecurity concerns, it's about protecting the entire digital ecosystem from fraudulent sites. While CISOs may see this as a secondary risk, it's a top priority for marketing and branding.

Mark Eggleston
CISO, CSC



Finance and procurement: cost-effectiveness, ROI, and insurance benefits

Financial decision-makers and procurement teams evaluate investments based on cost, efficiency, and measurable ROI. One effective way to demonstrate the financial impact of domain security risks is by pulling real-world examples from news headlines. Sometimes an action as simple as forwarding a link to a recent incident can help finance teams see the tangible consequences of underinvestment. A well-protected DNS may also reduce the rate of business disruptions, supporting financial stability.

Frame DNS security as a business enabler, rather than just a technical safeguard, and gain broader organizational support and ensure that DNS protections are treated as a strategic priority.

Proving ROI: building the business case for proactive DNS security

Securing investment in DNS security requires more than just highlighting risks, it involves demonstrating measurable financial and operational benefits. CISOs and cybersecurity leaders must translate security concerns into clear business value, showing how investing in DNS security reduces costs, streamlines operations, and minimizes financial exposure.

Security budgets don't always rise at the same pace as cyber risk. In CISO Outlook 2025, only 7% of respondents reported a significant budget increase from 2024 to 2025, while 80% reported a moderate increase.⁵

In this environment, DNS investments need to demonstrate measurable risk reduction and resilience for operations.

Reducing costs through risk mitigation and efficiency

A strong DNS security posture supports broader cyber risk reduction, which can help organizations maintain good standing with cyber insurance providers and align with widely accepted security frameworks. While cyber insurance policies don't typically offer DNS-specific discounts, strengthening domain protections demonstrates good cyber hygiene and reduces threats.

Organizations are also prioritizing repeatable, scalable methods, especially where speed of response matters. In CISO Outlook 2025, 50% of respondents said they have developed and regularly tested incident response plans, and 50% reported using an AI-based monitoring and enforcement solution.⁶ DNS security aligns with this shift toward operational maturity by improving visibility, accelerating mitigation, and strengthening continuity when disruptions occur.

Automation plays a key role in reducing the manual burden of domain security operations, from managing DNS configurations to monitoring for emerging threats and responding to incidents. It's also increasingly important for digital certificate management: as certificate life cycles shorten under CA/Browser Forum changes through 2029, organizations may need to renew secure sockets layer (SSL) and transport layer security (TLS) certificates far more frequently—averaging eight renewals per year in the future—making automated renewal workflows essential for preventing expirations and service interruptions.

Using financial models to quantify DNS risk

Executives and financial teams respond best to data-driven decision-making. Cyber risk quantification (CRQ) models, such as the annualized loss expectancy equation or the factor analysis of information risk (FAIR™) framework, help organizations estimate potential financial losses from DNS-related attacks, downtime, or DNS hijacking incidents. By applying these models, cybersecurity leaders can present concrete figures that demonstrate how proactive investment prevents far greater financial losses.

Conducting scenario-based risk assessments is another way to illustrate potential business disruption and financial impact caused by DNS failures. By modeling real world attack scenarios, organizations can visualize the hidden costs of a weak DNS security posture.

Enhancing threat intelligence and risk prioritization

Staying ahead of evolving threats requires continuous visibility into potential risks. Organizations that join industry-specific information-sharing groups, such as the National Council of Information Sharing and Analysis Centers, gain early warnings and insights into emerging DNS-related attacks.

Additionally, implementing continuous threat exposure management allows security teams to prioritize the most pressing DNS vulnerabilities, ensuring that resources are allocated efficiently to mitigate the highest-risk scenarios before they escalate.

Measuring cost savings with our DNS cost calculator

Understanding the financial benefits of DNS security requires clear cost modeling. The following DNS internal cost calculator provides a formula to help enterprises estimate the true cost of DNS downtime, factoring in variables such as lost transactions, remediation costs, and operational disruptions.

You don't need a complex model to estimate the value of DNS security. Once you map DNS downtime to real business impact—lost productivity, lost transactions, and recovery time—the ROI becomes much easier to justify.

Mark Flegg
Senior Director, Security Products and Services, CSC



DNS Cost Savings Calculator	Metrics
Number of staff to manage DNS	2
Yearly salary per staff member	\$75,000
Cost of benefits ~ 30% of staff cost	\$45,000
Yearly hardware, software, and bandwidth	\$40,000
Total cost of running internal DNS	\$160,000
Proposed cost of external DNS service	\$50,000
Total savings by using external DNS service	\$110,000

Note: actual numbers are examples.

By demonstrating quantifiable cost savings, operational efficiencies, and reduced financial exposure, cybersecurity leaders can build a compelling business case for DNS security investment, one that speaks directly to the priorities of executives, finance teams, and risk managers.

Making DNS security a business priority

DNS security is a critical yet often overlooked part of an organization's cybersecurity strategy. As this report has shown, the cost of DNS security failures extends far beyond downtime, including financial loss, regulatory penalties, and reputation damage.

Beyond implementing technical controls, CISOs and security leaders must communicate DNS security in business terms. By aligning messaging with executive priorities, quantifying risk, and demonstrating ROI, organizations can secure the investment needed to protect their digital assets.

Taking proactive steps to strengthen DNS security now can prevent costly incidents in the future. **Talk to CSC today about a tailored solution to safeguard your organization.**

 cscdbs.com

“**Here's how to achieve executive buy-in for cybersecurity in three steps:**

- 1** Build relationships—Understand executives' priorities and take a steady, strategic approach.
- 2** Speak their language—Frame cybersecurity as a governance issue. Use guidelines like those in the National Association of Corporate Directors (NACD).
- 3** Demonstrate progress—Use dashboards or other clear visuals to show the impact of security investments.

Mark Eggleston
CISO, CSC



 **Let's talk** 1 800 927 9800 | [cscdbs.com](https://www.cscdbs.com)

About CSC

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSecSM platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit [cscdbs.com](https://www.cscdbs.com).

¹CSC, *The CISO Outlook 2025, 2025*, <https://www.cscdbs.com/en/resources/2025-ciso-cybersecurity-outlook-report/>.

²Splunk, *The Hidden Costs of Downtime, 2024*, https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html.

³CSC, *The CISO Outlook 2025*.

⁴CSC, *The CISO Outlook 2025*.

⁵CSC, *The CISO Outlook 2025*.

⁶CSC, *The CISO Outlook 2025*.