DOMAIN & DNS

SECURITY, COMPLIANCE & PERFORMANCE

DISCUSSION BRIEF

> "Every company we audit discovers glaring security risks and compliance holes they didn't know existed, despite their belief that they had it covered."
>
> *PETER LAMANTIA, CEO, AUTHENTIC WEB INC*

DOMAIN DISASTERS IN THE NEWS

When people make mistakes, brands are damaged.
IT'S TIME TO LOCK IT DOWN.

READ MORE ABOUT THESE DISASTERS

CLICK HERE

DOMAIN AND DNS RISKS ARE REAL

Large enterprises are dependent on their mission-critical digital footprint and increasingly vulnerable to breaches, errors and omissions.

The news media can barely keep up with corporate disasters that include:

DOMAIN EXPIRY: Live domains stop working due to non-renewal.

DOMAIN HIJACKING: Unauthorized parties appropriate domains from the rightful owners.

DNS HACKS: Undetected system hacks compromise customer data and trust.

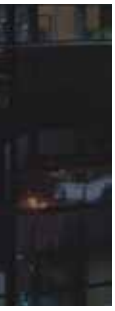
DOMAIN MISDIRECTS: An intended domain end-point gets re-pointed to unauthorized content.

FACT

The TOP TWO security & compliance threats to the enterprise come from:

#1 Disgruntled Employees

#2 Uninformed Employees



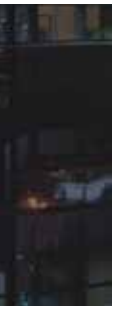
These are just a few examples of the infinite variables of domain and DNS-related mischief that can result in catastrophic consequences for your enterprise. When digital applications go down due to issues with the underlying domains, the brand and commercial fallout can be extreme.

FACT

Organizations that neglect Domain and DNS security and compliance WILL be targeted for exploits.

WHY DO CORPORATE DOMAIN DISASTERS HAPPEN?

Domain and DNS infrastructure is increasingly complex. Many Enterprise domain/DNS systems have evolved into a *"The Pyramid of Risk."* Having multiple registrars, name servers and thousands of configuration settings and end-points exacerbates the risk.



IS THIS REALLY A PROBLEM FOR YOUR COMPANY?

Very likely it is.

There are two ways you can confirm your exposure:

1. *A high level external audit.*
2. *Complete the checklist.*

CLICK HERE

MULTIPLE DOMAIN REGISTRARS

No centralized control. Hard to manage. → *ACCESS, CHANGE MANAGEMENT: EXPOSURE TO HIJACKS, THEFTS, CRITICAL SERVICE FAILURES.*

MULTIPLE DNS PROVIDERS

Proliferation of settings and access. Hard to manage. → *ACCESS, CHANGE MANAGEMENT: EXPOSURE TO COMPROMISED OR MISCONFIGURED SETTINGS & HACKS*

THOUSANDS OF ZONE FILES AND END-POINTS

Thousands of zone file resource records and no easy way to monitor all of them. → *CHANGE MANAGEMENT, VISIBILITY: EXPOSURE TO DNS CACHE POISONING, UNKNOWN NETWORK STATUS*

THE ISSUE: LACK OF SYSTEMS

BUSINESS RELIES ON PEOPLE.
Lack of systems to enforce security and compliance policies expose the enterprise. These risks are often hidden from stakeholders who lack a complete view to the ecosystem.

HOW DO YOUR DOMAIN/DNS SYSTEMS STACK UP?

Three important questions security & compliance officers need to ask

1. Do you have a unified, ***tamper-proof*** system to manage domains and the DNS ? ○ YES ○ NO ○ NOT SURE
2. Can you ***prove*** the system enforces security policy and change management? ○ YES ○ NO ○ NOT SURE
3. Is the system ***integrated*** with Registrar and DNS control systems? ○ YES ○ NO ○ NOT SURE

Your answers determine your vulnerability.
MOST ORGANIZATIONS ARE AT RISK.

STAKEHOLDERS AFFECTED

RISK OFFICERS
Lack visibility to DNS risks and systems to establish and enforce policies.

SECURITY SPECIALISTS
Understand risk but lack systems to enforce team member change actions.

IT STAFF
Are overworked with tasks. Domain and DNS security risks are not managed proactively.

DOMAIN ADMINISTRATORS
Lack compliance tools to enforce domain policies and monitor team activity.

DIGITAL MARKETERS
Lack DNS business intelligence data to measure and improve digital performance.

MORE FACTS

Companies struggle with legacy systems that do not provide ability to manage change and health.

Use of multiple domain registrars and DNS services increase business risk exposure.

Resource records have errors. Lack of visibility makes error states hard to detect and resolve.

Domains are a shared responsibility creating security and compliance accountability gaps.

HAVE YOU CONDUCTED A DOMAIN/DNS AUDIT LATELY?

Our audit will pinpoint your exposure

Our Domain and DNS audit includes an APEX-level resource record examination which can reveal larger zone file issues and security risk.

AUDIT CHECKS	*RISK LEVEL*
Multiple Domain Registrars	Severe
Multiple DNS Services	Severe
HTTP Status Codes	
200's	Low
300's	Moderate
400's	Severe

WHAT CAN AN AUDIT MEAN FOR YOUR ENTERPRISE?

Most organizations trust security, IT and administrative teams to address risk by brute force and will. Policies and procedures are often manual, non-system based and insufficient to protect your business and customers.

IF AN AUDIT FINDS THIS...	*THEN YOU ARE EXPOSED TO THIS*
Multiple Domain Registrar Services	Domain Hijack and Interruption
Multiple DNS Services	Domain Theft
HTTP Response Inspections	DNS Cache Poisoning
IP • DNSSEC • SPF	Compromised network endpoints

ENTERPRISE PRIORITIES

Security

Compliance

Performance

Protect your operation from catastrophic Domain/DNS incidents

1

Complete our DNS/Domain Operations Checklist

CLICK HERE

2

Contact Us for Your Domain/DNS Audit

SECURE YOUR DIGITAL BRAND

authenticweb.com

Contact Us | info@authenticweb.com | 1.855.436.8853