EPSTEIN
BECKER
GREEN

Protecting Your Domain Name System (DNS) Security To Avoid Data Loss & Insider Threat

Brian G. Cesaratto

August 27, 2019

Presented by

Brian G. Cesaratto
Member of the Firm
bcesaratto@ebglaw.com
212-351-4921

https://www.ebglaw.com/brian-g-cesaratto/

- Practice focuses on cybersecurity, risk assessments, information security programs, insider threat, incident response and computer forensic investigations.
- Cybersecurity best practices.
- Certified Information Systems Security Professional (CISSP)(awarded by ISC2).
- Certified Ethical Hacker (CEH) (awarded by EC-Council).
- Certified Common Security Framework (CSF) Practitioner (designation by HITRUST).

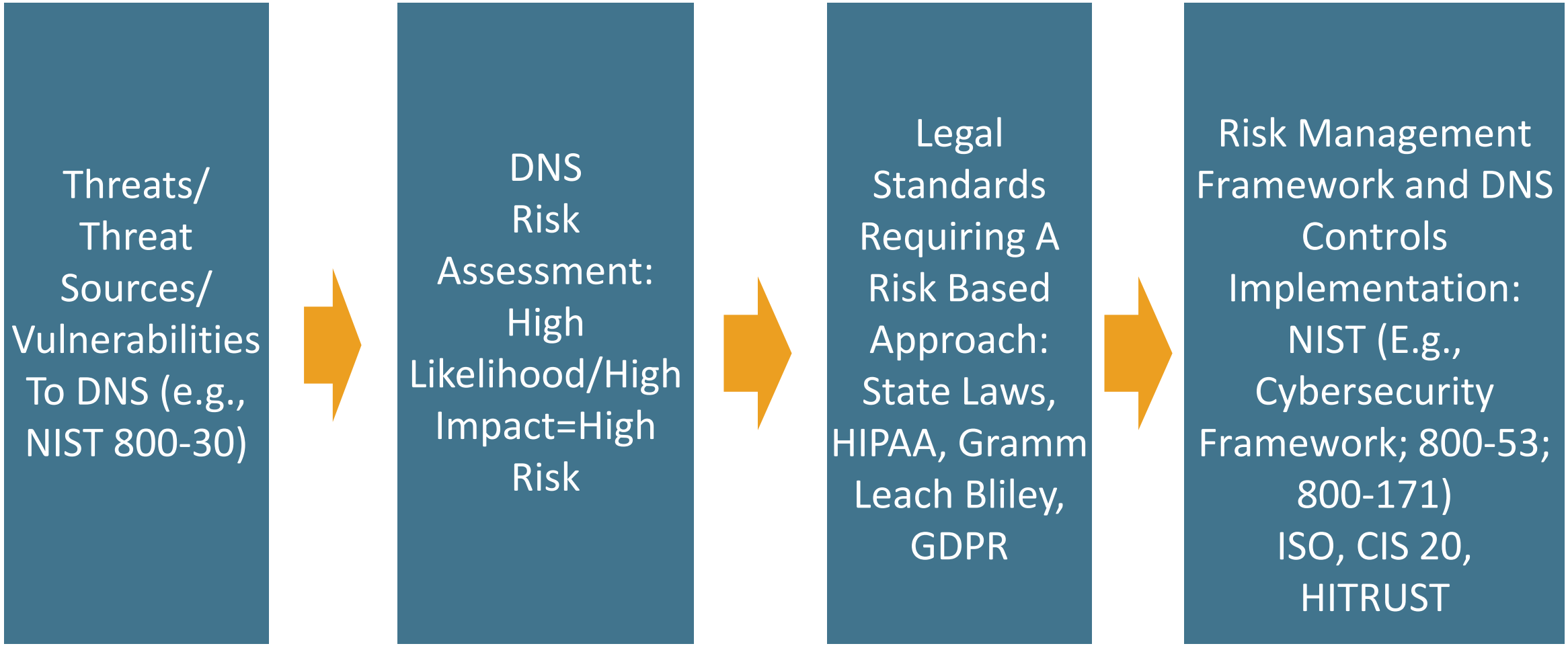
This presentation has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal, state, and/or local laws that may impose additional obligations on you and your organization.

Attorney Advertising

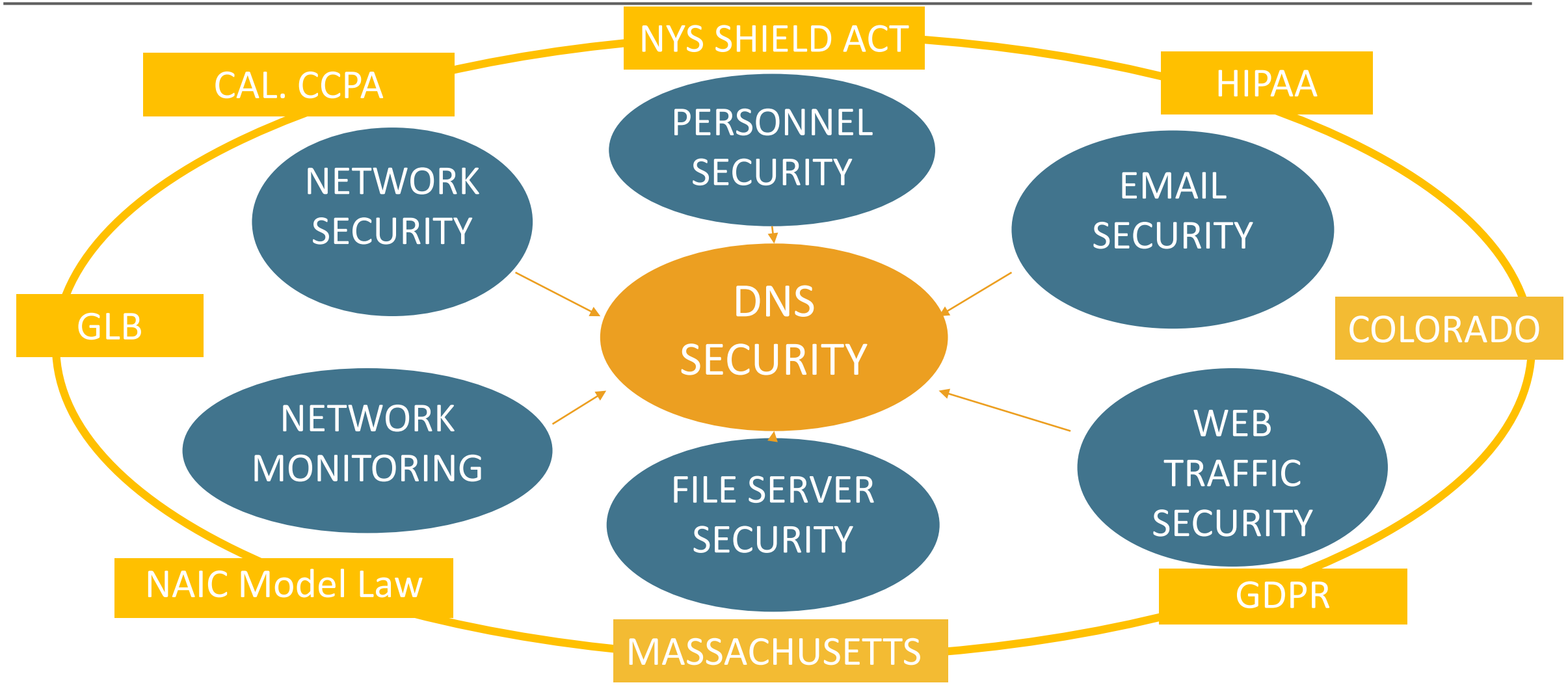
DNS Cybersecurity Is Everyone's Responsibility: Board, C-Suite, Legal, IT, HR, Compliance, Security

- NIST Guidebook: "Cybersecurity Is Everyone's Job."
- "We are the greatest vulnerability in any organization."
- "In this era of persistent cyber threats, an organization can be secure only with the active participation of everyone. Unfortunately, many organizations limit security responsibilities to designated security personnel that perform specialized security functions. Effective security must be enterprise-wide, involving everyone in fulfilling security responsibilities. Each member of the group, from the newest employee to the chief executive, holds the power to harm or to help, to weaken or strengthen, the organization's security posture."
- https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

Risk Assessment, Legal Cybersecurity Standards and Risk Management Framework To Address DNS Security



Breach of DNS Security Caused By A Failure In The Statutorily Mandated "Reasonable Safeguards" Is Likely To Have A High Impact

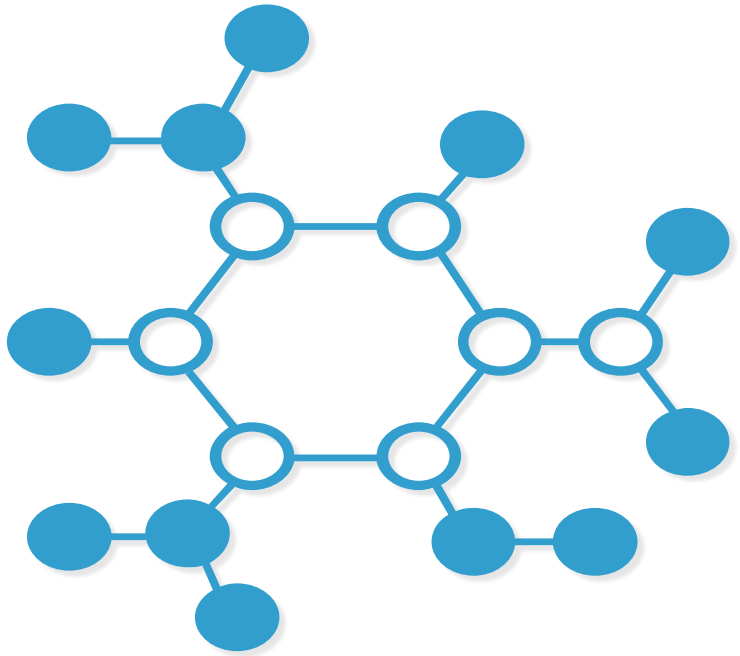


What is the Domain Name System (DNS)?

- DNS connects computers and routes access to resources.
- “Plumbing of the Internet.”
- Users remember domain names (www.anycompany.com).
- Computers use numbers (IP or Internet Protocol) to route traffic to a particular computer.
- DNS translates domain names (www.anycompany.com) into IP addresses (172.30.xxx.xxx) and back again.
- DNS informs the requesting computer of the unique numerical identifier expressed as a 32 bit number of the resource to be reached, and the transmission begins.
- Communications between computers on the Internet depend on DNS to get to their intended destination.

Why is DNS so very important to your organization?

- The importance of DNS to your organization's cybersecurity cannot be understated.
- Almost every communication, web request, online resources starts with a DNS inquiry – called a Query.
- Simplified terms: User's Computer to DNS: Where do I find the computer hosting the domain www.anycompany.com out there among the hundreds of millions of computers on the Internet?
- Where do I find the computer hosting the email server to reach the email address t.smith@anycompany.com?
- DNS returns the IP address assigned to the particular computer the user is looking for.

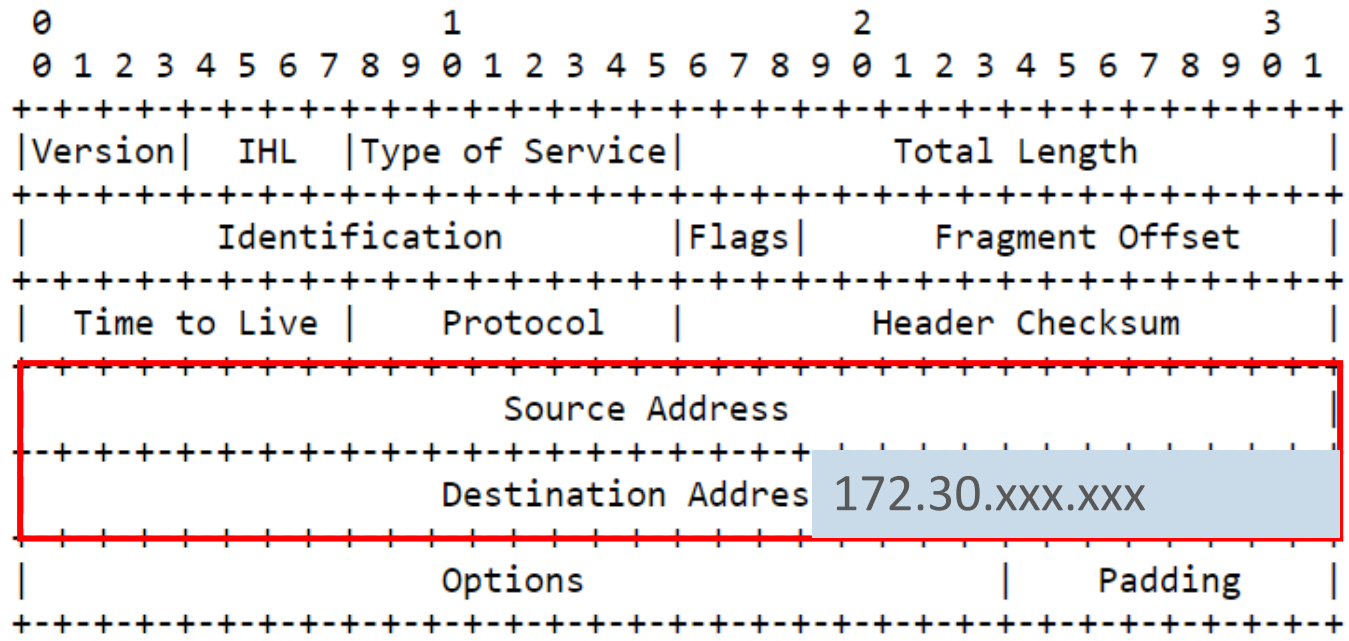


DNS Header: Query and Response

QUERY	RESPONSE
QUESTION: www.anycompany.com	QUESTION: www.anycompany.com
	ANSWER: 172.30.XXX.XXX

Requesting Computer Includes The IP address In IPv4 Header And Sends Off The Transmission

A summary of the contents of the internet header follows:



Example Internet Datagram Header

Organization's Registration of A Domain With A Registrar Results In The Creation of a "Who Is" Record.

- Look up "anycompany.com" https://whois.icann.org/en/about-whois
- Look up provides information concerning the organization and the associated domain.
- Technical and Contact Details including registrant name and organization.
- Also provides the Name Server (i.e., the computer) associated with the domain.
- ICANN oversees the assignment of IP addresses and domain names.
- Key Takeaway: If a hacker can modify your organization's Who Is account information, your traffic can be owned.

What Are The Elements Of The DNS Infrastructure At Risk?

- Domains are your organization's brand.
- Domains identify your organization on the Internet.
- Register your domains with a registrar so that no two organizations use the same domain.
- Who Is Lookup Record is created and associated with the domain.
- Account holder (Administrator) identifies the computer that authoritatively responds to DNS inquiry concerning the domain.
- Creation of key records: "A" record; "MX" record; "NS" record.

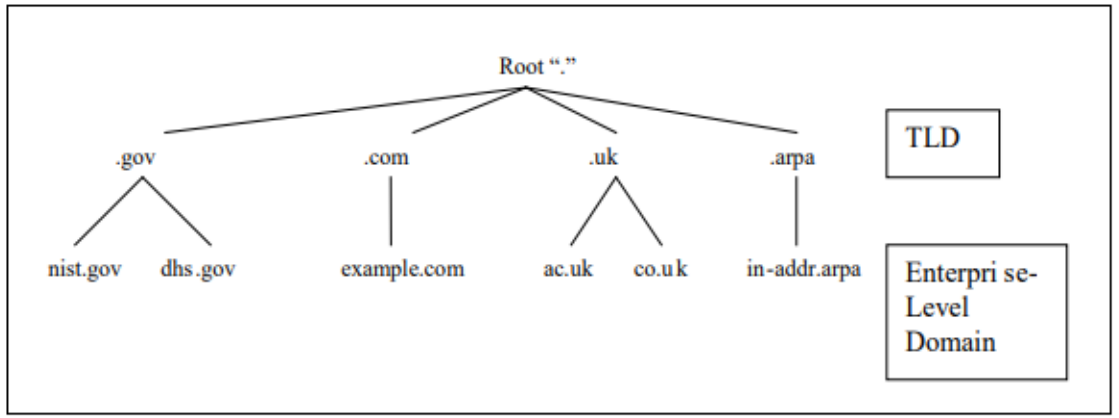


Figure 2-1. Partial DNS Name Space Hierarchy

Source - NIST – Secure DNS Deployment Guide

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

Why Is DNS Vulnerable To Threats?

- Public, Distributed and Flexible
- Public – To function, computers seeking information must be able to access the information across the Internet
- Distributed – Not one computer is responsible for operation , but distributed and administered to by computers all over the world
- Flexible: Organizations can change the name server associated with the domain name by changing the IP address associated with the domain name.
- DNS vulnerabilities are inherent in its purposes and operation

The Threats to DNS Are Longstanding and Growing With Significant Escalation In The Last Few Months

- **2007: ICANN Factsheet**:

  Root Server attack on 6 February 2007: “On 6 February 2007, starting at 4:00 a.m. PST, for approximately two and a half hours, the system that underpins the Internet came under attack.

  Three-and-half hours after the attack stopped, a second attack, this time lasting five hours, began.

  The core DNS servers of the Internet were hit with a significant distributed denial of service attack, or DDoS.”

  ICANN reported that 6 of the root servers were attacked with two badly affected.
  https://www.icann.org/en/system/files/files/factsheet-dns-attack-08mar07-en.pdf

The Threats to DNS Are Longstanding and Growing With Significant Escalation In The Last Few Months

- **2016: NY Times -** "Hackers Used New Weapons To Disrupt Major Websites Across U.S." – Reporting on distributed denial of service attack against DNS provider Dyn, causing users to be unable to reach customers' websites, including Twitter, Netflix, Spotify, Airbnb, Etsy, SoundCloud and the NY Times. Attackers used an overwhelming flood of DNS queries using thousands of Internet of Things (IoT) devices, like cameras, home routers and baby monitors to conduct a distributed denial of service attack. Dyn issued a statement: "Dyn confirms Mirai botnet as primary source of malicious attack. . . Attack generated compounding recursive DNS retry traffic, further exacerbating its impact." https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html; https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
- **Nov. 27, 2018**. **Cisco Talos** reports on DNS hijacking redirecting traffic of Middle East governmental websites and a Middle East airline company. The attackers redirected traffic to attacker controlled IP addresses. https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

The Threats to DNS Are Longstanding and Growing With Significant Escalation In The Last Few Months

- **Jan. 9, 2019**: **FireEye** researchers at Mandiant identify numerous DNS hijacking attacks (altering DNS records) affecting domains belonging to government, telecommunications and internet infrastructure across the Middle East, North Africa and North America. Mandiant reported: "While this campaign employs some traditional tactics, it is differentiated from other Iranian activity we have seen by leveraging DNS hijacking at scale." https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
- **Jan. 24, 2019**: **DHS** Emergency Directive 19-01/Director's Blog Post: "This **is the first** Emergency Directive issued by the Cybersecurity and Infrastructure Security Agency (CISA) under authority granted by Congress in the Cybersecurity Act of 2015. . . Because it's our responsibility to take actions to protect Federal systems, we felt an urgent response was required to address the risk." DHS Emergency Direction 19-01 - Mitigate DNS Infrastructure Tampering. https://cyber.dhs.gov/ed/19-01/
- **February 5, 2019**. **National Cyber Security Centre (UK)**: The NCSC is investigating a large-scale DNS hijacking campaign that has reportedly affected government and commercial organizations worldwide. The majority of the entities targeted are in the Middle East, but some impact has also been reported in Europe and the United States. https://www.ncsc.gov.uk/news/alert-dns-hijacking-activity

The Threats to DNS Are Longstanding and Growing With Significant Escalation In The Last Few Months

- **April 19, 2019**. **Cisco Talos** reports on a "new cyber threat campaign [calling it] Sea Turtle" involving state-sponsored DNS hijacking attack manipulating DNS systems, targeting national security organizations in the Middle East and North Africa and their providers. Cisco reported: "One of the most notable aspects of this campaign was how they were able to perform DNS hijacking of their primary victims by first targeting these third-party entities." https://blog.talosintelligence.com/2019/04/seaturtle.html
- **July 9, 2019. Cisco Talos** reports that the DNS hijacking campaign is not slowing down. https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html
- **July 12, 2019**. **UK National Cyber Security Centre** issued "Alert Ongoing DNS Hijacking and Mitigation Advice." In January 2019, NCSC published an alert to highlight a large-scale global hijacking campaign to hijack Domain Name System (DNS). . . . since the NCSC's alert in January further activity has been observed, with victims of DNS hijacking identified across multiple regions and sectors." https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice.

DHS Director's Blog Post – January 24, 2019

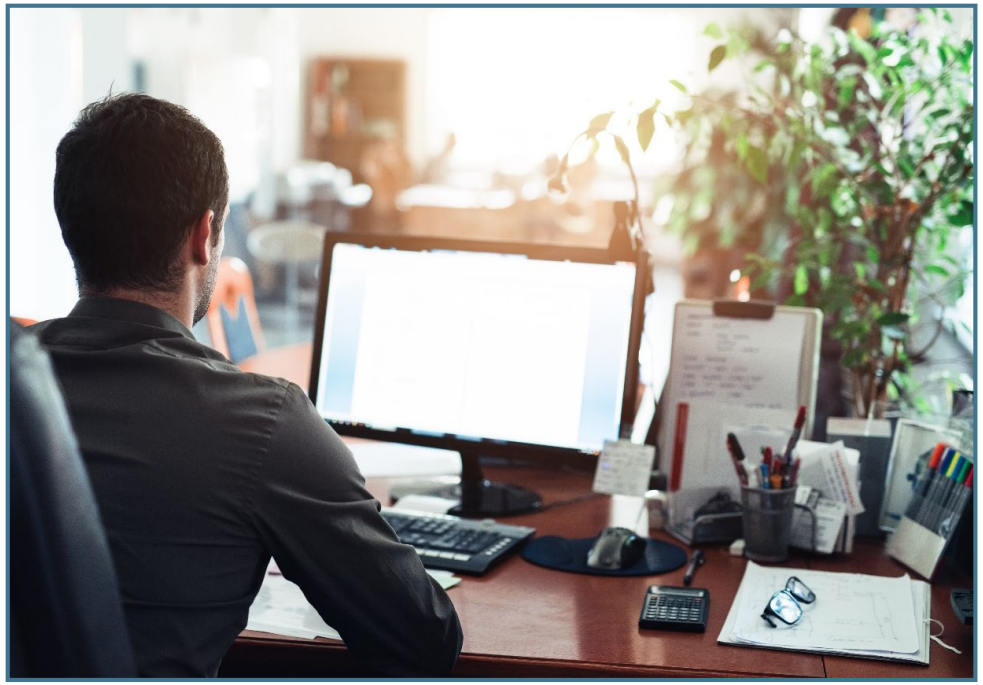
- **Why CISA issued our first Emergency Directive**
- ***By Christopher Krebs, Director***
- https://cyber.dhs.gov/blog/#why-cisa-issued-our-first-emergency-directive
- "**Like real life, if someone can change your address, lots of bad things can happen. The same is true of DNS**. "
- "In this case – as revealed by FireEye researchers a little over a week ago, with related reporting by Cisco Talos in late 2018 – malicious actors obtained access to accounts that controlled DNS records and made them resolve to their own infrastructure before relaying it to the real address. Because they could control an organization's DNS, they could obtain legitimate digital certificates and decrypt the data they intercepted – all while everything looked normal to users. "
- "**This is roughly equivalent to someone lying to the post office about your address, checking your mail, and then hand delivering it to your mailbox. Lots of harmful things could be done to you (or the senders) depending on the content of that mail.**"

MAJOR ATTACKS ON DNS

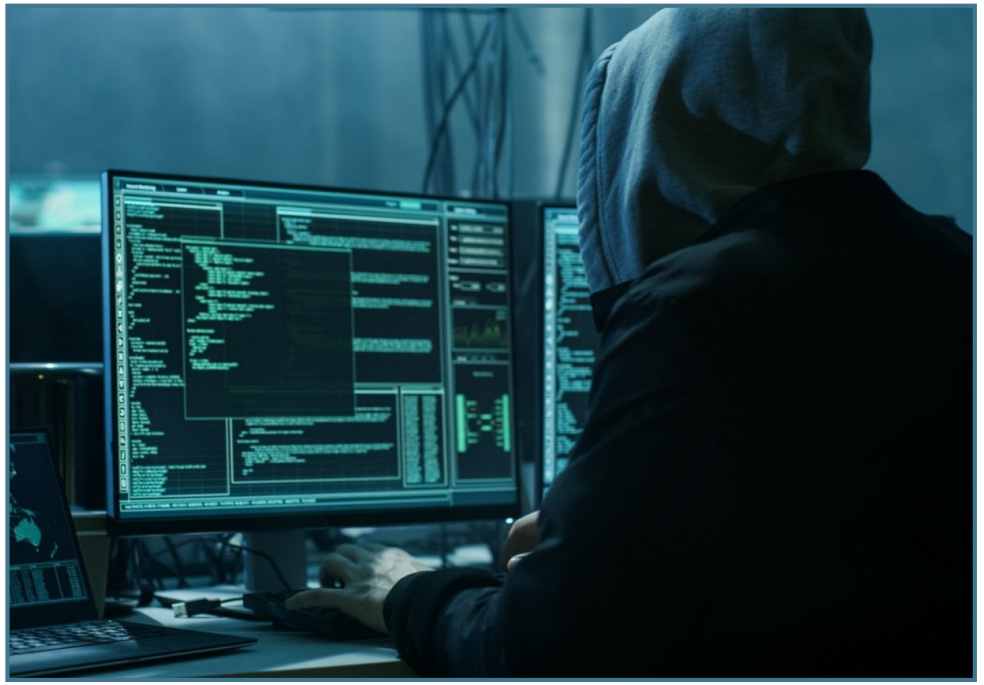
Presented by Brian G . Cesaratto

EPSTEIN BECKER GREEN

What are the Threat Sources to DNS?



Insider Threat



External Hacker

An Organization Cannot Comply With Applicable Legal Standards Requiring Reasonable Safeguards Without Considering Risks to DNS

- HIPAA – Health Insurance Portability and Accountability Act. 45 C.F.R. 164.308(a)(1)(i), (ii). Standard: Security Management Process. Implement Policies and procedures to prevent, detect, contain, and correct security violations. . . Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity or business associate."
- Gramm-Leach-Bliley Safeguards Rule. 16 C.F.R. 314.3: "Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."

An Organization Cannot Comply With Applicable Legal Standards Requiring Reasonable Safeguards Without Considering Risks to DNS

- California Civil Code 1798.81.5: "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
- NYS SHIELD Act: In order to achieve compliance, an organization must implement a data security program that includes: (i) "reasonable administrative safeguards" that may include designation of one or more employees to coordinate the security program, identification of reasonably foreseeable external and insider risks, assessment of existing safeguards, workforce cybersecurity training, and selection of service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract; "reasonable technical safeguards" that may include risk assessments of network, software design and information processing, transmission and storage, implementation of measures to detect, prevent and respond to system failures, and regular testing and monitoring of the effectiveness of key controls; and "reasonable physical safeguards" that may include detection, prevention and response to intrusions, and protections against unauthorized access to or use of private information during or after collection, transportation and destruction or disposal of the information.

An Organization Cannot Comply With Applicable Legal Standards Requiring Reasonable Safeguards Without Considering Risks to DNS

- NYS Department of Financial Services (NYSDFS) Cybersecurity Regulation 500: "Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technical advances."
- Massachusetts Standards For The Protection Of Personal Information. 201 CMR 17: Every person that owns or licenses personal information about a resident of the Commonwealth shall develop and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information.

An Organization Cannot Comply With Applicable Legal Standards Requiring Reasonable Safeguards Without Considering Risks to DNS

- Colorado Revised Statutes. 6-1-713.5. To protect personal identifying information, as defined in section 6-1-713(2), from unauthorized access, use, modification, disclosure, or destruction, a covered entity that maintains, owns, or licenses personal identifying information of an individual residing in the state shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations.
- GDPR. Art. 32. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

DNS Impacts: Network Security, Workforce Training and Logging/Monitoring

- **HIPAA Security Rule**. 45 CFR 164.308 and 164.312 – Administrative and Technical Safeguards: 164.308(a)(1)(i). Standard: Security Management Process. Implement Policies and procedures to prevent, detect, contain, and correct security violations. 164.308(a)(1)(ii). Implementation specifications. A. Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity or business associate. 164.308(a)(1)(ii). Implementation specifications. D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports. 164.308(a)(3)(i) Workforce Security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have [authorized] access from obtaining access to electronic protected health information. 164.312(a) (1) Standard: Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have granted access rights. 164.312(e)(1). Standard: Transmission Security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

DNS Impacts: Network Security, Workforce Training and Logging/Monitoring

- **Massachusetts: 17.04**. Computer System Security Requirements. Every person that owns or licenses personal information about a Massachusetts resident shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, to the extent technically feasible, shall have the following elements: (1) Secure user authentication protocols including: (a) control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (d) restricting access to active users and active user accounts only; and blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system; (2) Secure access control measures that: (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

DNS Impacts: Network Security, Workforce Training and Logging/Monitoring

- **Massachusetts 17.04** (cont'd) (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly. (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information; (5) Encryption of all personal information stored on laptops or other portable devices; (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information. (7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis. (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

DNS Impacts: Network Security, Workforce Training and Logging/Monitoring

NYSDFS. 500.03. Cybersecurity Policy. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: . . .(c) access controls and identity management; (f) systems operations and availability concerns; (g) systems and network security; (h) systems and network monitoring . . .

500.09. Risk Assessment. Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

500.12. Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

Risk Management Framework to Implement Administrative, Technical and Physical Controls To Protect DNS

- NIST Cybersecurity Framework (some of the controls applicable to DNS): "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Identify, Protect, Detect, Respond, Recover
- Identify: ID.GV 1-4: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environment, and operational requirements are understood and inform the management of cybersecurity risk.
- Protect: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
- Protect: PR.PT-4: Communications and Control Networks are Protected

Risk Management Framework to Implement Administrative, Technical and Physical Controls To Protect DNS

- Detect: DE.AE-1. A baseline of network operations and expected data flows for users and systems is established and managed.
- Detect: DE.AE-2. Detected events are analyzed to understand attack targets and methods.
- Detect: DE.AE-3. Event data are collected and correlated from multiple sources and sensors.
- Detect: DE.AE-4 Impact of events is determined.
- Respond. RS.AN-1: Notifications from detection systems are investigated.
- Recover. RC.RP-1: Recovery plan is executed during or after a cybersecurity incident

Risk Management Framework to Implement Administrative, Technical and Physical Controls To Protect DNS

- NIST 800-53 Controls
- System and Communications SC -20 – Secure Name/Address Resolution Service. Requiring authentication and integrity verification of the DNS query and response to assure the integrity of the host/service name to network address resolution information obtained through the service.
- System and Communications SC-21 – Secure Name/Address Resolution Service (Recursive or Caching Resolver). Requiring authentication and integrity verification of the DNS query and response exchanged by recursive resolving or caching domain name system (DNS) servers to assure the integrity of the host/service name to network address resolution information obtained through the service
- System and Communications C-22 – Architecture and Provisioning For Name/Address Resolution Service. The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
- System and Information Integrity SI-4 – Information System Monitoring. Requiring monitoring of the information system to detect attacks and potential attacks.

DNS Hijacking Campaign

January 24, 2019

The National Cybersecurity and Communications Integration Center (NCCIC), part of the Cybersecurity and Infrastructure Security Agency (CISA), is aware of a global Domain Name System (DNS) infrastructure hijacking campaign. Using compromised credentials, an attacker can modify the location to which an organization's domain name resources resolve. This enables the attacker to redirect user traffic to attacker-controlled infrastructure and obtain valid encryption certificates for an organization's domain names, enabling man-in-the-middle attacks.

https://www.us-cert.gov/ncas/alerts/AA19-024A

DNS Hijacking Campaign

Technical Details. Using the following techniques, attackers have redirected and intercepted web and mail traffic, and could do so for other networked services.

1. The attacker begins by compromising user credentials, or obtaining them through alternate means, of an account that can make changes to DNS records.
2. Next, the attacker alters DNS records, like Address (A), Mail Exchanger (MX), or Name Server (NS) records, replacing the legitimate address of a service with an address the attacker controls. This enables them to direct user traffic to their own infrastructure for manipulation or inspection before passing it on to the legitimate service, should they choose. This creates a risk that persists beyond the period of traffic redirection.
3. Because the attacker can set DNS record values, they can also obtain valid encryption certificates for an organization's domain names. This allows the redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.

https://www.us-cert.gov/ncas/alerts/AA19-024A

DNS Hijacking Campaign Mitigations

DHS recommended the following best practices to help safeguard networks against this threat:

- Update the passwords for all accounts that can change DNS records.
- Implement multifactor authentication on domain registrar accounts, or on other systems used to modify DNS records.
- Audit DNS records to verify they are resolving to the intended location
- Search for encryption certificates related to domains and revoke any fraudulently requested certificates.

https://www.us-cert.gov/ncas/alerts/AA19-024A

DNS Hijacking Campaign Mitigations

National Cyber Security Centre recommended the following best practices to help safeguard networks against this threat:

- Registrar Security – "The most common DNS hijacking takes place at the registrar level, simply by gaining unauthorized access to a registrant's account. "
  - Phishing prevention and deploy multi-factor authentication when available
  - Regularly audit who can access the registrar control panel and make changes
  - Ensure contact information at registrar is up to date and accurate
  - Use a registrar with a registrar lock service. Prevents domain from being transferred without additional authentication.
  - Monitor for unauthorized domain transfers and unauthorized activity.

https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice

.

DNS Hijacking Campaign Mitigations

- DNS Security for nameservers
  - Limit Zone Transfers
  - Strict access control measures for those with access to DNS infrastructure
  - Monitor SSL certificates
  - Consider implementing DNSSEC
  - Monitor zone files for unauthorized domain transfers and unauthorized activity.
- Web Application Security
  - Monitor access or authentication logs to detect attacker based on IP address.

https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice

DNS Hijacking Campaign Mitigations

- Industry trends in failing to implement Registry Lock services.
- CSC Global reports:
  - 2019: 57% of media brands surveyed do not implement registry lock because registry lock is unavailable or not activated. https://www.cscdigitalbrand.services/en/cyber-security-report/
  - 2017: Only 16% of insurance providers and 32% of financial sector organizations surveyed use registry lock because registry lock is unavailable or not activated. https://www.cscdigitalbrand.services/blog/august-cyber-security-report-financial-and-insurance-sectors-among-the-most-targeted-industry/

Other Side of The Equation: Monitoring DNS – A Tool To Combat Insider Threat

- Enable DNS Logging
- Adopt Written Well-Publicized Employee Monitoring/System Use Policies
- Policies should provide that all system usage is monitored and no expectation of privacy by employees
- Courts have held that there is an expectation of privacy and limits on an employer's ability to monitor employee system usage in the absence of such notice. See, e.g., *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010).
- Employee activities fully revealed through DNS logs – websites/cloud resources they connect to as long as the organization has visibility into those devices and connections.
- Early indicator of insider threat.

Most Data Breaches Are Caused by Insiders —Whether Intentionally or Inadvertently*

Insiders caused

Network Attacks Targeting Healthcare Data (IBM Security, "Security trends in the healthcare industry: Data theft and ransomware plague healthcare organizations")

68%

Patient Health Record Privacy Violations (Protenus, "31 Health Data Breaches Disclosed in January as HHS Fines for Late Reporting")

59%

Attacks in Financial Services (IBM Security, IBM X-Force Threat Intelligence Index 2017)

58%

*Ponemon Institute Research Report, 2016 Cost of Insider Threats: Benchmark Study of Organizations in the United States.

Enable DNS Logging As An Early Warning Of Insider Threat Insider Case Studies – Malicious Insiders

- ***United States v. Sazonov*** (No. 1:17-cr-00657) (SDNY 2018) (Financial Services)
  - **Trading Platform** – analyze data and automatically implement trading strategies
  - **Insider** (software engineer) – Looking for new employment opportunities
    - Over a decade with the Firm
    - Used his privileged access to software repository and downloaded source code into a zip file
    - Copied it and encrypted a second zip file
    - Ran searches on how to use steganography
    - Broke up the zip file and appended it to innocuous files on his desktop using steganography (including his personal tax and immigration documents)
    - Had emails with the files attached ready to go heading into employment termination meeting
    - Before meeting, uploaded the encrypted zip file to a file sharing platform
    - Also, printed out a hard copy of the source code
    - Was not allowed back to desk after termination meeting per policy

Insider Case Studies – Malicious Insiders (cont.)

- ***United States v. Seoung Jeon*** (No. 1:14-MJ-00054) (D. Del. 2015) (Manufacturing)
  - Engineer for a clothing manufacturer of concealment fabric
  - Following a negative performance review and after being advised he would not be receiving a compensation increase, used his work computer to download over 800 files and folders from a restricted drive he had access to as a member of the engineering team.
  - Transferred the files to external hard drives and other storage media.

Key Takeaways – DNS Risk and Mitigation

- Cybersecurity Risk Management Requires Engagement/Ask Questions and Get Answers.
- Cybersecurity is a Team Effort: Board, Legal, HR and Compliance should engage with IT, IT Security, and Physical Security.
- Conduct a Formalized Risk Assessment: Consider Risks to DNS Based On Anticipated Threats. This is a foundational requirement and your best protection. Consider conducting risk assessment using legal counsel to protect communications concerning cybersecurity under attorney client privilege.
- Implementing Statutorily Mandated Reasonable Cybersecurity Safeguards should be informed by a risk assessment. Same holds true to protect key technologies and trade secrets.
- Depending On Results Of Risk Assessment: Reduce risk by implementing administrative, technical and physical measures to protect DNS using a Risk Management Framework.
- Conduct cybersecurity training to protect DNS: anti-phishing and social engineering training is a must.
- Implement complex passwords and multifactor authentication for DNS administrators to prevent unauthorized changes to DNS records.

Key Takeaways – DNS Risk and Mitigation

- Use Secure Registrars providing visibility into your domains with domain locks and multi-factor enabled.
- Patch DNS servers and applications pursuant to formalized configuration management program.
- Implement a formalized system to monitor/proxy DNS traffic to ensure DNS is being used as intended.
- Monitor and audit DNS logs to verify that queries are resolving to intended locations.
- Monitor your organizations “A” and “NS” records.
- Monitor DNS/Use DNS Firewalls to block attacker domains – e.g., Domain Generated Algorithm domains.
- Monitor encryption certificates to your domains so you are alerted to unauthorized changes.
- Implement written polices and procedures around protecting DNS, including configuration management, passwords, monitoring and incident response.
- Use DNS monitoring as part of an Insider Threat Management Program. Gives visibility into websites and cloud resources accessed by employees. Part of formalized program to protect against data loss.

Key Takeaways – DNS Risk and Mitigation

- Consider implementing DNSSEC (which builds trust in the DNS query and resolution process) if technically feasible.
- Consider DNS backup services.
- Retain records showing your organization owns the domain for purposes of restoring ownership in the event a domain is hijacked.