THE 2024 HEALTHCARE CYBER TREND RESEARCH REPORT

Infoblox Product Marketing
January 2024

TABLE OF CONTENT

HEALTHCARE CYBERATTACKS BREACH OVER 118.9 MILLION PATIENT RECORDS IN 2023

We are pleased to announce the release of our 2024 Healthcare Cyber Trend Research Report. Recognizing the critical need for timely intelligence to protect patient data and healthcare operations, we share our data and perspectives on the barrage of cyberattacks experienced by the healthcare industry in 2023 and their ongoing impact on this vital sector.

We also share our view on important defense-in-depth (DID) strategies and key cyber defense technologies such as domain name system detection and response (DNSDR). These strategies and tools can help reduce risk and increase the resilience of healthcare cyber defense ecosystems.

> “In 2023, per our analysis of HHS/OCR data, there were an estimated 118.9 million healthcare patient records compromised by cyberattacks within the United States. This alarming number corresponds to about 35.38 percent of the projected U.S. population of 335,893,238, estimated by the U.S. Census Bureau in January 2024.
>
> This statistic is truly staggering.
>
> It suggests that, even with some individuals having their personal healthcare records stolen from multiple databases, that perhaps more than a third of the U.S. population had their healthcare records breached in 2023 alone.
>
> We expect that our healthcare institutions will continue to be subjected to unyielding attacks from organized crime groups and nation-states. These opponents are intent on extorting money through ransomware and exploiting a growing variety of malware, phishing, and social engineering strategies. We don’t anticipate this trend to reverse anytime soon.”
>
> Anthony James
> Vice President, Product & Solutions Marketing
> Infoblox

The results of this healthcare research are summarized as follows:

- New data extracted from the HHS/OCR HIPAA database, as available on January 4, 2024, shows 697 major data breaches in 2023. This includes the loss of paper files and other breach sources that may not be attributable to Hacking/IT. Further, note that this data may be subject to adjustments and changes over time.
- Of these 697 data breaches, approximately 551 were explicitly attributed to hacking or IT incidents. These numbers represent incidents reported under HIPAA that affected 500 or more patient healthcare records.
- The 551 data breaches in 2023 due to Hacking/IT Incidents included an estimated 118.9 million patient records.

The responsible healthcare organizations (covered entities) report data breaches under the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule (CFR 164.400-414), which requires HIPAA-covered healthcare entities and business associates to provide notification following a breach of unsecured protected health information (PHI) affecting 500 or more individuals.

Our research documents statistics about these data breaches specifically categorized as Hacking/IT (cyberattacks), and we refer to them as major data breaches. These major breaches are found and extracted from the U.S. Department of Health & Human Services Office of Civil Rights (HHS/OCR) database. HHS/OCR does not release the data-on-data breaches caused by Hacking/IT where fewer than 500 patient records are compromised.

If a breach of unsecured protected health information impacts 500 or more individuals, there is a requirement that the affected entity must notify the Secretary without undue delay, and certainly no later than 60 calendar days from the discovery of the breach. In the case of a breach affecting fewer than 500 individuals, the entity must notify HHS/OCR within 60 days of the end of the calendar year in which the breach was discovered. However, the entity is not obligated to wait until the end of the year to report breaches affecting fewer than 500 individuals; they may report such breaches as soon as they are discovered. While the entity can report all breaches affecting fewer than 500 individuals on a single date, a separate notice must be completed for each breach incident. Please note that our research only includes major data breaches affecting over 500 individuals reported in the calendar year 2023 as of the date of the extracted report.

Our research team has reviewed a variety of information sources in preparing this report, including:

- The accessible databases maintained within the HHS/OCR; and,
- Information published on the Internet by recognized sources, press releases and announcements provided by the impacted reporting organizations.

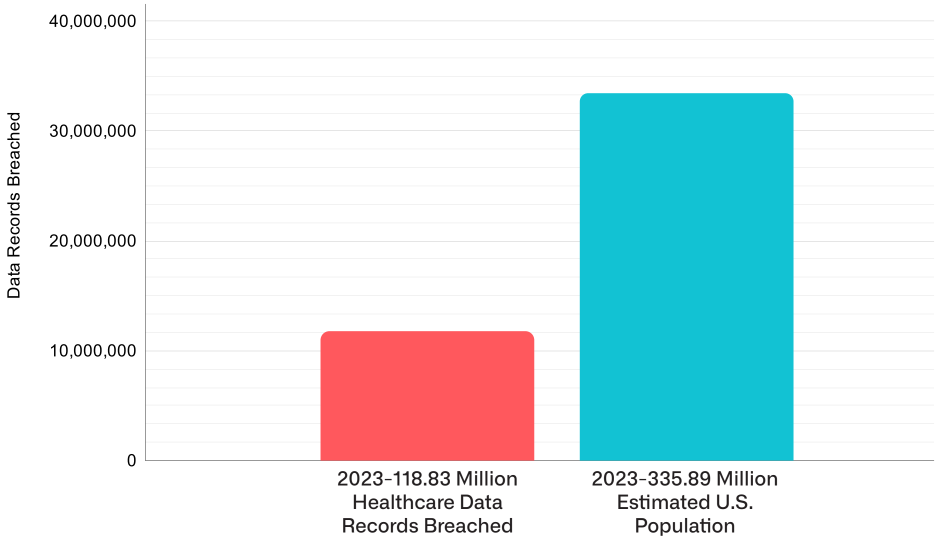
One of our contributing authors has very specific experience that includes implementing and managing a HIPAA compliance program in a digital health company. Our reviewers include technical team members who are also subject matter experts in domain name system detection and response (DNSDR) and core network services. These subject matter experts are frequently involved with industry best practices using DNS to secure healthcare enterprise networks.

DATA ANALYSIS

Our initial analysis required us to extract and review data from within the HHS/OCR database for reported breaches during 2023. The focus of this report is solely within the cyber security domain, so all of our attention went to reviewing data categorized as Hacking/IT within the HHS/OCR database.

Graphic 1 – U.S. Healthcare Records Breached by Cyberattack in 2023 Versus the Total U.S. Population

U.S. HEALTHCARE RECORDS BREACHED DUE TO CYBERATTACK VS. U.S. POPULATION



U.S. HEALTHCARE RECORDS BREACHED DUE TO CYBERATTACK VERSUS U.S. POPULATION

Graphic 1 above illustrates the number of healthcare data records breached throughout 2023 versus the United States' total population as estimated in January 2024 by the Bureau of the Census. This data reflects a total of 118,834,964 records breached versus the total estimated U.S. population of 335,893,238.

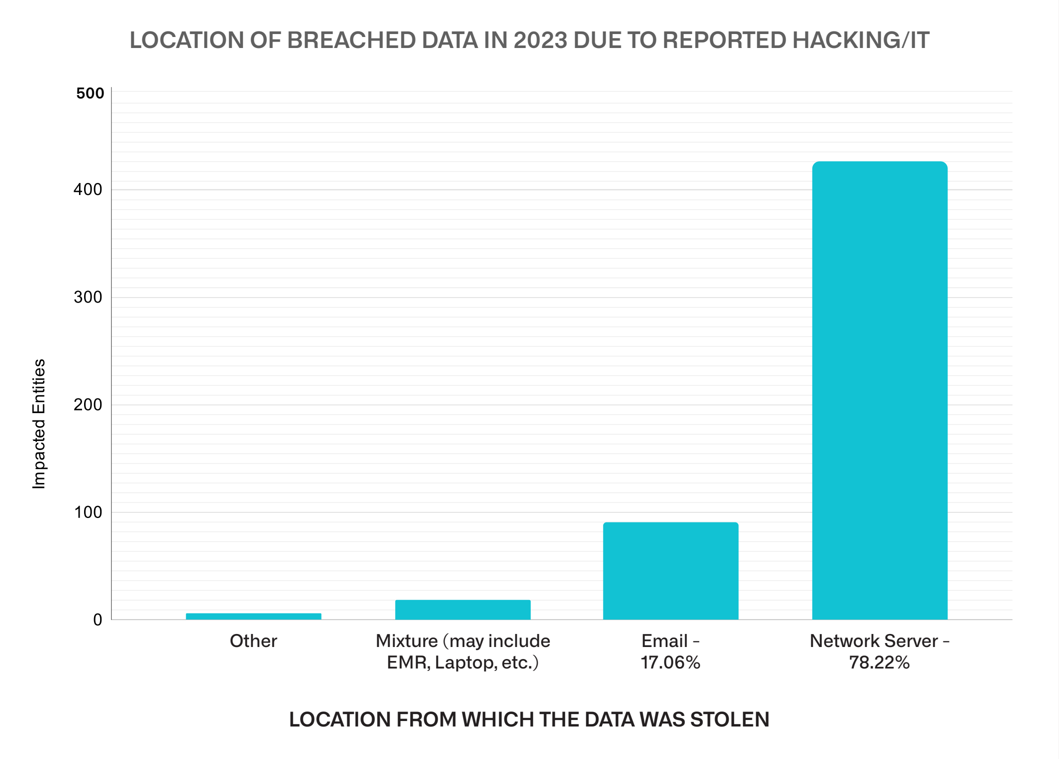
If we assume no overlap of patient data records breached, the total percentage would be 35.38 percent of the U.S. population — meaning, about 1 in 3 U.S. citizens had their personal healthcare data breached in a cyberattack in 2023.

Given this data, the average size of a major data breach for Hacking/IT, as reported in 2023, is approximately 215,671 patient data records per data breach event.

LOCATION OF BREACHED DATA

Upon review of the 2023 major healthcare data breaches due to Hacking/IT, in about 78% of the attacks, the breached data was in one or more network servers.

Graphic 2 – Location of Breached Data in 2023 Due to Reported Hacking/IT



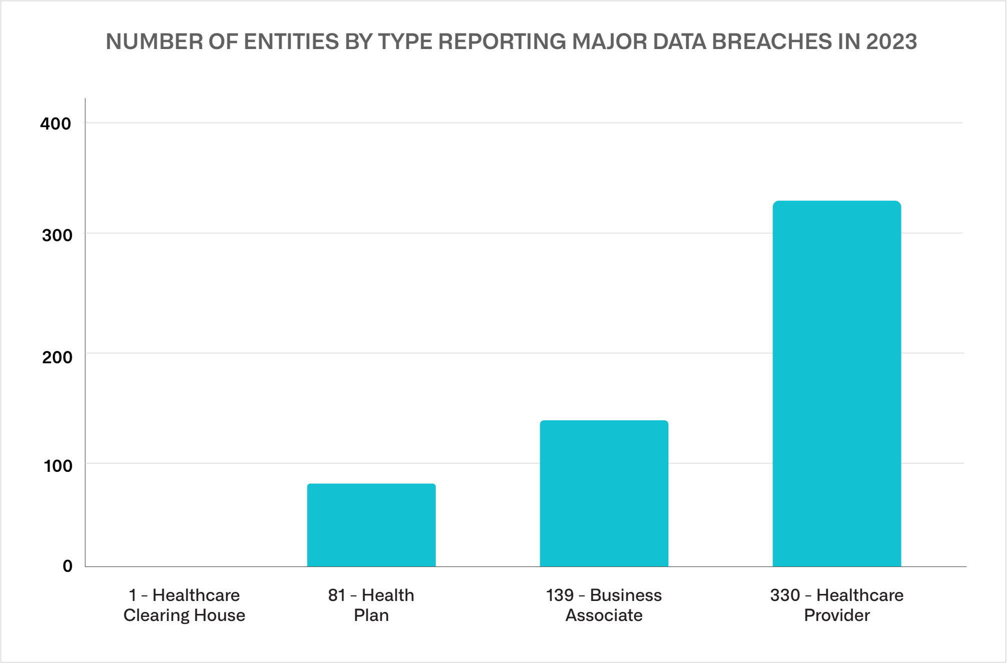
Location of Breached Data	Impacted Entities	Percent
Other (not identified)	6	1.09%
Mixture (may include EMR, Laptop, etc.)	20	3.63%
Email	94	17.06%
Network Server	431	78.22%
TOTAL	**551**	**100.00%**

TYPES OF REGULATED ENTITIES REPORTING MAJOR DATA BREACHES

Upon review of the 2023 major healthcare data breaches due to Hacking/IT, over 25% of the major data breaches were reported by business associates. A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.[1]

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Graphic 3 – Number of Entities by Type Reporting Major Data Breaches in 2023



Entity Type	Reporting Entities	Percent
Healthcare Clearing House	1	0.18%
Health Plan	81	14.70%
Business Associate	139	25.23%
Healthcare Provider	330	59.89%
TOTAL	**551**	**100.00%**

HEALTHCARE ON THE FRONTLINES: EVOLVING DEFENSE-IN-DEPTH TO COMBAT CYBER THREATS

The healthcare industry has embarked on a significant digital transformation journey in recent years, driven by the promise of cost reduction, improved patient outcomes, and enhanced care delivery. While these efforts unlock considerable financial and technological advantages, they also inadvertently expand the attack surface for malicious actors.

Cybercriminals see the healthcare sector as a lucrative target, drawn by its vast size, reliance on technology, treasure trove of sensitive data, and critical vulnerability to disruptions. Protecting these organizations demands a robust defense-in-depth approach, layering multiple physical, technical, and administrative security controls to create overlapping shields against digital assaults. Building a complete defense-in-depth strategy maximizes resilience against ever-evolving cyberattacks.

While defense-in-depth's importance is paramount, healthcare organizations often lack the resources and expertise needed for effective implementation. Keeping up with ever-changing security patches, securing funding for cutting-edge solutions, and staffing qualified personnel to manage complex systems often fall short. These vulnerabilities leave enticing openings for cybercriminals.

Building a Fortress: Essential Technology in Healthcare's Defense-in-Depth Armor

A comprehensive defense-in-depth strategy necessitates multiple security layers, encompassing physical, technical, and administrative controls. Here are some crucial technologies critical for large healthcare organizations:

1. **Firewalls:** The gatekeepers of your network, meticulously inspecting and filtering incoming and outgoing traffic to prevent unauthorized access.
2. **Intrusion Detection & Prevention Systems (IDPS):** Vigilant sentinels monitoring network activity, identifying suspicious patterns, and proactively thwarting cyberattacks.
3. **Extended Detection & Response (XDR):** Shields individual devices from malware and other digital threats, acting as shielding for every endpoint. Extended Detection and Response (XDR) is a security platform that monitors, detects, and responds to threats across your cybersecurity environment with consolidated telemetry, unified visibility, and coordinated response. XDR has a broad scope, offering integrated security across a wider range of products, from networks and servers to cloud-based applications and endpoints.
4. **Domain Name System Detection & Response (DNSDR):** A multifaceted tool capable of identifying and tracking DNS queries, blocking a wide range of DNS-based attacks, detecting and stopping unknown malicious activities, and orchestrating automated remediation through integrated systems. DNSDR leverages threat intelligence to sharpen its detection capabilities, allowing you to stay ahead of evolving attackers and their infrastructure.
5. **Data Encryption:** The ultimate security vault, scrambling sensitive data into an unreadable form, accessible only to authorized users.
6. **Access Controls:** Selective gatekeepers, requiring user authentication before granting access to sensitive data, ensuring unauthorized access attempts are met with a firm no.
7. **Security Information & Event Management (SIEM):** SIEM collects and analyzes security data from across your network, enabling swift detection and response to cyber threats.
8. **Vulnerability Scanning:** The tireless scout, uncovering weaknesses in your network and applications before they become exploitable targets, allowing for timely remediation.
9. **Patch Management:** The constant guard, diligently ensuring software and systems are always up to date with the latest security patches, minimizing attack vulnerabilities.
10. **Backup and Recovery:** The safety net, protecting critical data from loss in the event of a cyberattack or other disasters, providing a swift path to restoration.
11. **Employee Training:** The human firewall, empowering employees to recognize and respond to cyber threats, understand secure use of technology, and become active participants in your security posture.

Synergy is Key: Layering Technologies and Controls

These technologies work best when implemented in a layered approach, creating overlapping defensive walls. However, relying solely on technology is a gamble. Healthcare organizations must also establish robust administrative and physical controls – policies, procedures, and training – to ensure the effectiveness of their security measures.

By adopting a multifaceted approach to cybersecurity, prioritizing a complete defense-in-depth strategy, and continuously strengthening their defenses, healthcare organizations can stand stronger against cyber threats and safeguard the sensitive data entrusted to them. This increased resilience helps ensure the safety and privacy of patients, their information, and, ultimately, the trust they place in your care.

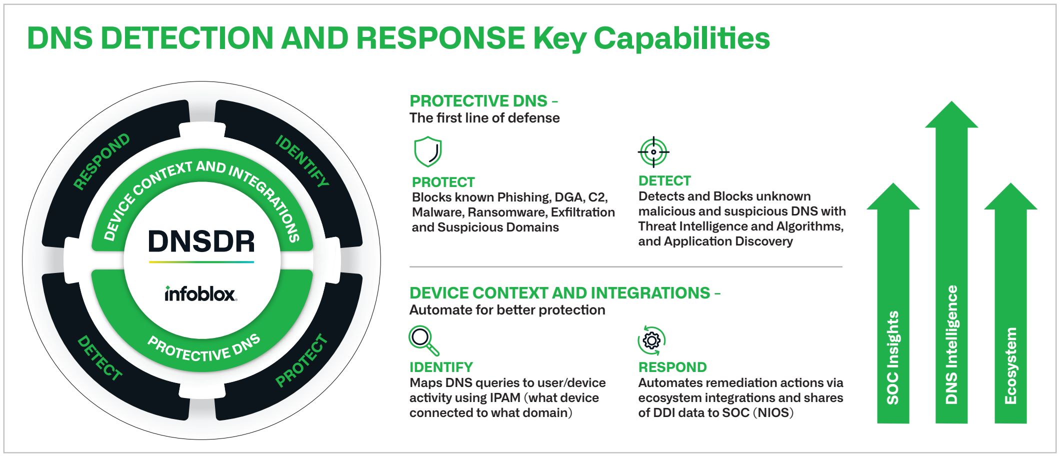
> *"Our analysis highlighted that using secure DNS would reduce the ability for 92% of malware attacks both from command and control perspective, deploying malware on a given network.[2]"*
>
> Anne Neuberger
> **Director of the Cybersecurity Directorate**
> **National Security Agency**

DNSDR: GUARDING HEALTHCARE NETWORKS AGAINST EVOLVING THREATS

DNSDR can help healthcare organizations improve their cyber resiliency by providing several important capabilities. By monitoring DNS queries, DNSDR can identify suspicious activity such as DNS tunneling, domain spoofing, and DNS cache poisoning. DNSDR can also be used to block the distribution of malware, phishing, and illegal content before they even reach the end user.

Leveraging a complete ecosystem is essential. DNSDR is designed to integrate with and work with other security tools and systems, allowing for automated remediation and response. By leveraging DNS threat intelligence, DNSDR can help organizations stay ahead of emerging threats and protect their networks more effectively. It encompasses several expanded and robust core capabilities that help improve the resiliency and efficacy of your cyber defense ecosystem and deliver value.

Graphic 4: Infoblox DNS Detection and Response



DNS DETECTION AND RESPONSE Key Capabilities

PROTECTIVE DNS – The first line of defense

PROTECT Blocks known Phishing, DGA, C2, Malware, Ransomware, Exfiltration and Suspicious Domains

DETECT Detects and Blocks unknown malicious and suspicious DNS with Threat Intelligence and Algorithms, and Application Discovery

DEVICE CONTEXT AND INTEGRATIONS – Automate for better protection

IDENTIFY Maps DNS queries to user/device activity using IPAM (what device connected to what domain)

RESPOND Automates remediation actions via ecosystem integrations and shares of DDI data to SOC (NIOS)

The Five Pillars of DNSDR: Bolstering Network Security

1. **Identify: Mapping the Network Landscape**
    - Function: Correlates DNS queries with user/device activity through IP Address Management (IPAM) and DNS-based application discovery.
    - Benefit: Comprehensive network understanding of who and what generates DNS queries, enabling faster security triage and reduced Mean Time to Respond (MTTR) by helping to pinpoint compromised assets more accurately without sifting through multiple logs.

2. **Protective DNS: Shielding Against Cyber Threats**
    - Function: Blocks various threats like phishing, ransomware, malware C&C, DGA, data exfiltration, suspicious domains and more. It also filters content and employs DNSSEC for system-wide protection, including IoT and OT devices.
    - Benefit: Prevents malicious activities from impacting the network, minimizing potential damage and disruption.

3. **Detect: Proactive Defense Against Emerging Threats**
    - Function: Leverages DNS threat intelligence and AI/ML algorithms to identify and block unknown malicious DNS activities.
    - Benefit: Strengthens proactive defenses against evolving threats, allowing early detection and prevention of potential intrusions.

4. **Respond: Automated Remediation and Rapid Response**
    - Function: Triggers automated response workflows through ecosystem integrations with Security Operations Center (SOC) tools, leveraging DDI data for swift action.
    - Benefit: Quicker and more effective response to detected threats, potentially interrupting the kill chain and mitigating the risk and potential data breach damage.

5. **DNS Threat Intelligence: Predicting and Thwarting Attacks**
    - Function: Utilizes data science, DNS expertise, and AI/ML capabilities to gather infrastructure-centric threat intelligence, identifying and tracking attacker infrastructure and evolving threat actors.
    - Benefit: "Pre-crime" domain blocking, preventing numerous attacks before they can even be launched.

DNSDR: Multifaceted Benefits Across Cyber Security Domains

DNSDR, through its key use cases, offers a multitude of benefits across various domains. DNSDR offers robust capabilities beyond its technical features, providing tangible benefits. It plays a crucial role in mitigating cyberattacks and minimizing critical risks like sensitive data breaches, brand reputational damage, and operational disruptions.

DNSDR's core strength lies in rapidly detecting and interrupting the DNS-driven kill chain, effectively stopping attacks earlier in the Kill Chain before they can inflict harm. This proactive approach significantly reduces the potential for damage and data loss. Furthermore, DNSDR demonstrably reduces the burden on Security Operations Centers (SOCs) by automating various security tasks related to threat detection, investigation, and understanding. This allows SOC teams to focus on strategic initiatives and improve overall security posture.

DNSDR use cases include:

1. **DNS is a Single Enterprise-Wide Control Point** to cover a broad attack surface, including on-premises, cloud, IoT/OT, remote workers, and branches.

2. **Block known bad traffic** using protective DNS capabilities to detect threats early and offload downstream security devices.
3. **Monitor DNS for misuse** using streaming analytics for detecting data exfiltration and DGAs.

4. **Identify attacker infrastructure** and block attacks pre-crime using infrastructure-centric threat intelligence.
5. **User and device attribution** to provide more than just the IP address of a compromised device, including device type, user name, network location and historical IPs.
6. **Enrich security tools** with DNS data and automatically trigger responses to events.
7. **Digital brand protection** to identify lookalike domains and take down offending domains fast with domain mitigation service.

Infoblox: Pre-Empting Threats with Early Domain Detection

Risk analysis forms the cornerstone of any effective cyber defense strategy, particularly in healthcare. However, our research shows a concerning gap between identifying and remedying security threats in healthcare organizations. Recent attacks compromising patient records highlight the urgent need for faster and more effective responses.

While many mid-size healthcare providers rely on legacy solutions or their local ISP for DNS, this approach leaves them exposed. In 2023, cybercriminals continued to exploit vulnerabilities in DNS, the crucial service that translates web addresses into the numeric codes that enable internet connectivity.

DNSDR offers a potent solution. By meticulously monitoring DNS activity, DNSDR can identify and block malicious or suspicious access attempts before they reach your network. This proactive approach bridges the security gap, allowing for timely remediation and improved safeguarding of sensitive patient data.

Implementing DNSDR now is no longer optional but critical to protecting your organization against evolving cyber threats. Don't let your risk analysis gather dust - embrace DNSDR and build a robust shield around your healthcare IT infrastructure.

Legacy DNS security controls leave critical gaps in healthcare security. Infoblox DNS Early Detection, a core component of DNSDR, offers a potent solution. Infoblox employs unique techniques to identify suspicious domains weeks or months before traditional intelligence feeds identify them as malicious. This proactive approach allows healthcare institutions to disrupt attacker timelines by blocking malicious domains early on, significantly reducing risk and potential damage.

Infoblox's early detection goes beyond merely identifying threats; it allows for proactive defense. By stopping potential attacks before they unfold, healthcare providers can prevent malware downloads, data exfiltration, and other harmful activities. This proactive "pre-crime" approach also streamlines security operations, minimizing investigation time and helping healthcare institutions outpace evolving threats and safeguard sensitive patient data.

CISA AND HHS ANNOUNCE CYBER TOOLKIT FOR HEALTHCARE

On October 25, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS) jointly hosted a roundtable discussion. This discussion focused on the cybersecurity challenges faced by the U.S. healthcare and public health (HPH) sector and how collaboration between government and industry can help bridge the gaps in resources and cyber capabilities.

Before the roundtable, CISA and HHS unveiled a cybersecurity toolkit, including resources specifically designed for the healthcare and public health sectors.

[2] https://executivegov.com/2020/06/anne-neuberger-on-nsas-secure-dns-pilot-program/

This cybersecurity toolkit includes:

- **Cyber Hygiene:** The toolkit starts with fundamental cyber hygiene steps every organization and individual should take.
- **Strengthening Defenses:** It provides industry best practices and resources on training, incident response planning, priority telecom services, cyber resilience, tackling ransomware, and more to help healthcare organizations strengthen their defenses.
- **Addressing Resource Constraints:** The toolkit acknowledges the resource constraints faced by the nation's healthcare systems and providers, especially since the start of COVID-19, and provides remedies to give sector stakeholders a greater ability to assess vulnerabilities and implement solutions proactively.
- **Collaborative Effort:** The toolkit is a result of a collaborative effort between CISA, HHS, and the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group.

The toolkit is designed to help organizations within the HPH sector build their cybersecurity foundation and internal processes to strengthen their defenses and stay ahead of current threats.

2023 LEGISLATIVE ACTIVITY ON HEALTHCARE CYBER SECURITY

In 2023, there were several significant legislative activities proposed related to healthcare cybersecurity:

Health Care Providers Safety Act of 2023: H.R. 286 was introduced on January 11, 2023, with the aim of enhancing the physical and cyber security of healthcare providers' facilities, personnel, and patients. The act[34] proposes authorizing grants to healthcare providers to pay for necessary security services and enhancements, such as video surveillance camera systems, data privacy enhancements, and structural improvements. This legislation reflects the growing importance of cybersecurity in the healthcare sector and the government's efforts to address these challenges. It provides healthcare providers with the resources they need to protect their facilities, personnel, and patients from physical threats and cyber threats.

Cybersecurity Act of 2023 (S. 2251): S. 2251 is a significant piece of proposed legislation that aims to enhance the cybersecurity practices of federal agencies. The act[56] would update the Federal Information Security Modernization Act (FISMA) to require federal agencies to report all cybersecurity incidents and conduct standardized cybersecurity procedures regularly. It also would codify the responsibilities of the federal Chief Information Security Officer and direct the Cybersecurity and Infrastructure Security Agency to study cyber threats to rural hospitals.

The estimated budgetary effects of the act would mainly stem from reporting and responding to cyber incidents at federal agencies, contracting with information security service companies, providing cyber incident response training to federal employees, hiring information security analysts, and developing training resources for rural hospital employees. However, there are areas of significant uncertainty, including anticipating the adoption schedules of new cybersecurity procedures and programs and predicting the staffing and contracting requirements of federal information security offices.

[3] https://www.govtrack.us/congress/bills/118/hr286

[4] https://www.congress.gov/bill/118th-congress/house-bill/286/text

[5] https://www.congress.gov/bill/118th-congress/senate-bill/2251

[6] https://www.govtrack.us/congress/bills/118/s2251

This act reflects the government's desire to improve cybersecurity practices within federal agencies and protect sensitive information from potential threats.

HC3 2023 Q1 Healthcare Cybersecurity Bulletin: The HC3 2023 Q1 Healthcare Cybersecurity Bulletin provides a comprehensive overview of the cyber threats faced by the Healthcare and Public Health (HPH) community in the first quarter of 2023. The bulletin[7] observed a continuation of many ongoing trends with regard to cyber threats to the HPH community, including ransomware attacks, data breaches, and often both together, which continued to be prevalent in attacks against the health sector. Ransomware operators continued evolving their techniques and weapons to increase extortion pressure and maximize their payday. For example, Emotet malware, a prolific threat to the health sector, went operational again in early March after being offline for three months. Vulnerabilities in software and hardware platforms, some ubiquitous and some specific to healthcare, continued to keep the attack surface of healthcare organizations open. Managed service provider compromise continued to be a significant threat to the health sector, as did supply chain compromise. The bulletin also highlighted industry reports of interest, such as the end of support for Microsoft Exchange Server 2013 and Windows Server 2012. This bulletin reflects the growing importance of cybersecurity in the healthcare sector and the government's efforts to address these challenges.

HEALTHCARE CUSTOMERS USING DNSDR

Anonymous Case Study from 2023 – A Leading Hospital and Level II Trauma Center

A leading hospital and Level II trauma center with a broad continuum of healthcare services decided to acquire a comprehensive and modernized DDI solution. Their current infrastructure involved using another vendor solely for IPAM, with no DNS integration or DHCP connections. A legacy solution was used to provide DNS services, and other DNS tools were essentially managed as a large spreadsheet.

After recognizing the potential for enriched threat intelligence tools through the combination of DDI and threat data, the acquisition of BloxOne Threat Defense became a top priority. The hospital team had confidence that BloxOne Threat Defense would significantly improve their DNS security by providing a complete DNSDR solution, thereby reducing the risks posed by numerous threat actors targeting the healthcare industry.

The hospital team used Infoblox to recognize the potential for greater efficiency in their security stack and tools. With a large number of IoT-connected devices such as MRI machines and the gaps in operating system level visibility, they believe that Infoblox will provide a return on investment (ROI) over time.

Anonymous Case Study from 2023 – A Large Health System in the United States

An integrated nonprofit health system with thousands of team members serving patients at a large network of hospitals and over 1,000 care locations experienced multiple attacks including phishing and DDoS. The healthcare leader was increasingly concerned about data security. Their team recognized that DNSDR could provide comprehensive security throughout the entire organization, regardless of user, device, or workload. They concluded that DNSDR represented a crucial defense-in-depth layer for efficient and effective protection.

[7] https://www.hhs.gov/sites/default/files/hc3-healthcare-cybersecurity-bulletin-q1-2023.pdf

Despite significant investments in security technologies, existing solutions could not deliver effective threat defense at the DNS level. Other controls had limitations, mainly because they were not actual DNS resolvers and thus couldn't effectively act on DNS-related information or provide comprehensive enforcement capabilities.

It became clear that they needed a solution like Infoblox DNSDR to bridge this gap. The visibility provided by Infoblox's telemetry and the details associated with each detection, such as DNS tunneling, offered previously unattainable insights. Lastly, Infoblox's ecosystem integrations and automation capabilities ensured that the necessary context was delivered rapidly and effectively within the SOC.

THE HEALTHCARE CYBER THREAT LANDSCAPE: A PERSISTENT CHALLENGE

The dramatic surge in patient data breaches in 2023 underscores that our institutions will continue to be prime targets in 2024. Cybercriminals, driven by the wealth of detail in healthcare data for identity theft and fraud, persist in their attacks. Furthermore, nation-states may also be implicated as they seek information for political or economic gains.

The expanding regulatory landscape intensifies the pressure on healthcare providers to meet compliance requirements. However, the immediate impact of proposed legislation, which aims to incentivize security enhancements, is lacking. As governments grapple with regulating the industry towards sufficient defense, the responsibility ultimately lies with individual institutions to safeguard sensitive data and patient privacy.

Despite ongoing investments in cybersecurity, data breaches continue to occur. The industry faces the enormous task of fending off sophisticated and well-funded threat actors. The escalating frequency of breaches and associated legal costs underscore the pressing need for robust defense strategies.

Infoblox DNSDR: A Proactive Approach to Reduce Risk and Strengthen Your Defense-in-Depth Ecosystem

Infoblox DNSDR emerges as an important solution for healthcare institutions. By offering deep visibility into DNS traffic, DNSDR empowers security teams to identify and neutralize potentially malicious activities before they compromise systems. Infoblox's advanced technology and expertise provide healthcare institutions with the means to protect sensitive data, maintain network integrity, and navigate the evolving threat landscape more effectively.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240207v1