CYBERSECURITY READINESS PODCAST SERIES

Episode 108

The Invisible Foundation: Why DNS Security Is the Governance Gap No One Is Watching

with Scott Harrell, President and CEO, Infoblox

Host	Dr. Dave Chatterjee, Duke University
Guest	Scott Harrell, President and Chief Executive Officer, Infoblox
Topic Focus	Foundational Network Infrastructure Security and the DNS Governance Gap
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 108 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Scott Harrell — President and Chief Executive Officer of Infoblox and former leader of Cisco's $20 billion enterprise networking business — to examine one of the most consequential security blind spots in modern enterprise governance: the foundational network infrastructure layer that every other security investment depends on, and that almost no organization actively governs.

The episode opens with the October 2025 Amazon Web Services outage, in which a single automated misconfiguration in a core routing service triggered a global cascade that took down AI services, financial platforms, and consumer applications worldwide, producing an estimated $581 million in losses. The cause was not a sophisticated cyber attack. It was a governance decision that had never been made — nobody was actively watching the foundational layer. That event becomes the opening frame for a conversation about DNS, DHCP, and IP address management: the three-part infrastructure, collectively known as DDI, that gives every device an address, translates every application name into a network location, and routes every piece of digital traffic to its destination. When it works, it is invisible. When it fails — or when an attacker exploits it — everything built on top of it stops.

Harrell's central argument is structural: 92% of all malware relies on DNS for its initial call-out to attacker-controlled infrastructure. The first thing any malware does when it lands on a network is resolve a malicious domain — and if that DNS request is blocked, the entire incident cascade never occurs. The payload is never downloaded. Lateral movement never begins. Privilege escalation never follows. The problem is that most enterprise security stacks are built to detect and respond to malware after it has activated — not to intercept the first domain resolution that enables everything that follows. This is the difference between reactive and preemptive security, and it is a governance choice that shows up in budget allocations: currently, only 5% of enterprise security spending goes to preemptive activities, with 95% consumed by detection and response. Gartner projects that organizations will need to reach a 50/50 split by 2030.

The conversation addresses how to make the governance case for foundational infrastructure investment, what differentiated DNS security looks like, how agentic AI is about to make network complexity exponentially harder to manage, and what three metrics every senior leader should be

demanding from their security teams. Analyzed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) Framework, the episode reframes network infrastructure security from an IT operational matter into a board-level governance imperative. The episode's core message is neither technical nor vendor-specific: the organizations that will withstand the next breach are not those with the most sophisticated detection tools — they are those that have decided to govern the layer everything else depends on.

Discussion Highlights

The Opening Incident: When the Foundation Fails

Dr. Chatterjee opens with the October 2025 AWS outage — a misconfiguration in a core routing service that produced $581 million in estimated losses and knocked out some of the world's most widely used platforms. Harrell uses the incident to illustrate what he describes as a systemic overestimation of digital resilience: most organizations believe their cloud dependencies provide resilience, when in reality they represent dependency. If the foundational infrastructure the cloud provider controls goes down, the organization's digital operations go down with it. The organization had no direct line of sight into the layer that failed.

> *What this incident illuminates is how brittle most environments actually are. People overestimate their resilience to a cyber attack, they overestimate their resilience to a network flaw. A lot of organizations do not understand where their critical points of failure are. Something as basic as DNS caused $581 million in damage — and most people, even after it happened, did not realize that was the root cause.*
>
> **— Scott Harrell, President and CEO, Infoblox**

Why the Foundational Layer Is the Last Thing Anyone Governs

Harrell identifies the root cause of foundational infrastructure neglect as a failure of leadership understanding, not technical competence. Organizations have historically run DNS, DHCP, and Active Directory on the same Windows servers because that is how it has always been done — and because no one in leadership has asked whether that is an acceptable configuration from a governance standpoint. The most common path to change, Harrell observes, is a new leader arriving from an organization that ran a purpose-built DDI platform and refusing to accept the legacy approach. Until that moment of recognition, the risks are invisible.

Dr. Chatterjee explicates DDI for the audience: DNS translates application names into network addresses (the iPhone contacts book analogy); DHCP assigns addresses to every device that joins the network; IPAM maintains an organization-wide inventory of what devices have what addresses and who is responsible for them. Together, these three services form the connective tissue of the digital enterprise. When they are healthy and governed, they are invisible. When they are exploited or fail, nothing built on top of them works.

> *The really informed boards, after CrowdStrike, started to ask: where are my mission-critical services, and do I actually understand what they are? Major telecom providers came to us and said: what we realized is that DNS and what you do is a Tier Zero service. If it doesn't work, the security doesn't work, the network doesn't work, the apps don't work. Nothing works.*
>
> **— Scott Harrell, President and CEO, Infoblox**

Turning the Network Into a Security Sensor

Harrell describes how DNS, because of its universality, is the single most powerful preemptive security control available to any enterprise. Every device — Windows, Mac, IoT, server, AI agent — uses DNS for every outbound connection. By monitoring and governing at that layer, a single policy can protect the entire enterprise. More importantly, it is the layer at which attacker infrastructure can be tracked proactively: Infoblox observes domains as they are registered, and convicts malicious domains an average of 68 days before they appear in any other threat intelligence feed, because the company monitors attacker infrastructure rather than waiting for malware to activate and propagate.

Last year, 25 million new malicious domains were registered. Of those, 24 million were unique to a single enterprise — meaning 96% of malicious domains observed were already targeted at a specific organization before they were used. This mass personalization of attacks, Harrell argues, makes detection-and-response models fundamentally insufficient. The only approach that can keep pace is one that tracks threat actor infrastructure before it is weaponized.

> *92% of all malware is going to leverage DNS. The first thing it does when it lands on the network is call out to a malicious domain. If I can stop it right there, at the network layer, before it downloads its payload, before it moves laterally, before it does privilege escalation — none of the rest of the incident happens. The network infrastructure itself is the best place to do that, because everything uses DNS. Everything.*
>
> **— Scott Harrell, President and CEO, Infoblox**

The 95/5 Problem: Why the Industry Is Built Backwards

One of the episode's most striking data points: only 5% of enterprise security budgets are currently spent on preemptive activities. The remaining 95% goes to detection, response, and recovery — the reactive model. Harrell is direct about the implication: an industry in which nearly every security company's product begins its work after malware has activated is an industry structurally oriented toward response rather than prevention. Gartner projects this ratio must shift to 50/50 by 2030, representing tens of billions of dollars in reallocation.

The litmus test Harrell offers is simple: if a vendor's value proposition begins after malicious software has landed on the network, it is reactive — regardless of how it is marketed. Preemptive security begins before the malware is weaponized, by tracking the infrastructure that threat actors use to operate, not just the malware they deploy.

> *Think about the security companies you know. How many of them are on the reactive side? If the work really starts after a malicious piece of software has landed in the environment, they are reactive. Period. It doesn't matter what they call themselves. And today, only 5% of the enterprise security budget is spent on preemptive activities. That has to change.*
>
> **— Scott Harrell, President and CEO, Infoblox**

Agentic AI and the Exponential Complexity Problem

Harrell introduces a data point that reframes the scale of the governance challenge ahead: according to recent Cisco research, an AI agent performing the same task as a human generates approximately 450

times the network traffic. An organization of 3,000 people that deploys thousands of agents has, in practice, doubled or tripled its digital workforce overnight — and with it, the number of network identities, connection endpoints, and potential intrusion points. Classical detect-and-respond architectures were not built for this scale.

Dr. Chatterjee reinforces the point: agentic AI does not merely increase traffic, it increases dependency. When business-critical workflows run on chains of agents, even latency degradation — not just outages — can crash processes in ways that operators may not detect in real time. The governance imperative is not just to secure the agents themselves, but to ensure the foundational infrastructure they depend on is resilient, governed, and monitored continuously.

> *You now have thousands of agents in the company. Think of them as digital humans — you've doubled the size of your workforce. But an agent creates 450 times the traffic of a human doing the same task. The complexity of the environment you are trying to secure is not going to change a little. It is going to go up exponentially. And your ability to save the patient using classical detect-and-respond is going to go down exponentially as that complexity rises.*
>
> **— Scott Harrell, President and CEO, Infoblox**

The CPD Framework Applied to DNS and Foundational Infrastructure Governance

Dr. Chatterjee applies the Commitment–Preparedness–Discipline (CPD) Framework to foundational infrastructure governance, observing that as Harrell described the conditions for genuine network security, each CPD pillar came alive in turn:

CPD PILLAR	APPLICATION TO DNS AND FOUNDATIONAL INFRASTRUCTURE GOVERNANCE
COMMITMENT	DNS governance begins with a leadership decision — not an IT ticket. Commitment means senior leaders claiming explicit ownership of foundational infrastructure security as a strategic business priority, not delegating it invisibly to network operations. It means understanding that the resilience of the organization's entire digital stack, including AI agents, cloud services, and security tools, depends on a layer that most leaders have never examined. Commitment requires actively asking: Where are our mission-critical services? What are our single points of dependency? What would it cost us if this layer failed for six hours? These are governance questions, and the answers must drive resource allocation.
PREPAREDNESS	Preparedness means building the operational capability to see, govern, and defend the foundational network infrastructure layer before an incident forces visibility. This includes deploying DNS security that monitors outbound connections in real time — intercepting malicious domain resolutions before payloads are delivered — maintaining an accurate IP address inventory, and ensuring that DHCP and DDI services run on purpose-built, resilient infrastructure rather than legacy Windows servers co-located with Active Directory. In the age of agentic AI, preparedness also means anticipating that every AI agent creates a new identity, a new address, and a new potential intrusion point, and that network traffic will grow exponentially as a result.

DISCIPLINE	Discipline is what separates a one-time infrastructure audit from a continuous security posture. It means measuring the right things — not just whether an outage occurred, but how long detection and recovery would take if the foundational layer failed; what percentage of known indicators of compromise the organization would have prevented proactively; and whether the ratio of reactive to preemptive security spending is shifting toward the 50/50 target that Gartner has identified for 2030. Discipline also means enforcing network segmentation, reviewing DNS threat intelligence continuously, and treating the fundamentals — DDI governance, routing integrity, access controls — as non-negotiable disciplines that survive budget cycles, leadership changes, and the next vendor pitch.

> *As I'm listening to you, I literally can hear these three pillars of security governance come alive. Commitment — actively engaged senior leadership that treats foundational infrastructure as a strategic priority, not a delegated IT task. Preparedness — the operational capability to govern the DDI layer, detect threats at the DNS layer before they activate, and anticipate the implications of agentic AI. Discipline — sustained, consistent execution of the fundamentals: the eating right, the exercising, the vitamins — every day, regardless of whether the last audit was clean.*
>
> **— Dr. Dave Chatterjee**

What Good Looks Like: Three Metrics for the Board

Harrell closes with a three-part metrics framework designed for non-technical leadership — questions that any board member or C-suite leader can ask their security team today, and that will reveal whether the organization is genuinely preemptive or merely reactive in disguise.

First, speed: How fast are new sanctioned services being rolled out? Which workflows are taking the longest, and what is being done to eliminate those friction points? In an age when attackers move at machine speed, an organization that cannot deploy sanctioned infrastructure faster than it deployed it five years ago is falling behind.

Second, proactive prevention rate: Of the new indicators of compromise published this month, how many would the organization have blocked proactively — before they became known? Can the team demonstrate that capability with evidence? If not, the security posture is not preemptive, regardless of what the dashboard shows.

Third, detection and recovery speed: How fast can the organization detect a foundational infrastructure failure — whether from misconfiguration, breach, or supply chain compromise — and reroute or recover? What are the single points of dependency, and how resilient is the organization if any one of them fails?

> *The metric I would ask the team: every month, new known indicators of compromise are published. How many of them would you have prevented proactively — before they became known? Prove it to me. Show me how. Because if you can't show me that, then your security posture is not preemptive, no matter what you call it.*
>
> **— Scott Harrell, President and CEO, Infoblox**

Actionable Recommendations

RECOMMENDATION	DETAIL
Commission a DNS Security Assessment	Before selecting a tool, map your exposure. Identify what percentage of your outbound DNS traffic is being inspected today. Understand whether your DDI infrastructure is running on dedicated, purpose-built systems or on legacy Windows servers co-located with Active Directory. The answer will tell you your current blast radius if the foundational layer is compromised.
Tier Your Infrastructure by Mission Criticality	Not all infrastructure is equally critical. Identify the systems whose failure would cascade — identity, DNS, core routing, AI agent orchestration — and treat these as Tier Zero services requiring the highest governance rigor, redundancy, and continuous monitoring. Board members should be able to name these services and articulate the recovery time objective for each.
Shift to DNS-Layer Threat Interception	Security investments that wait for malware activation are, by definition, reactive. Deploy DNS security that intercepts malicious domain resolutions before payloads land — not after. With 92% of malware relying on DNS for call-out, stopping the first outbound connection is the highest-leverage preemptive action available to any enterprise security team.
Rebalance Reactive vs. Preemptive Spending	If 95% of your security budget is spent on detection and response, your organization is gambling on response time. Gartner projects that organizations will need to reach a 50/50 split between preemptive and reactive security investment by 2030. Begin tracking this ratio now, and use it as a board-level governance metric alongside more conventional security KPIs.
Demand Proactive Metrics from Your Security Team	Ask monthly: Of the new indicators of compromise published this period, how many would we have blocked proactively? If we had not, how far could an attacker have moved through our environment before containment? These questions are not technical — they are governance questions. Requiring evidence-based answers to them changes team behavior, investment priorities, and incident outcomes.
Prepare Your Infrastructure for Agentic AI Scale	Each AI agent introduced into operations creates a new identity, a new IP address, and a new potential intrusion point. A 3,000-person company with thousands of agents already has more digital identities than human employees. Ensure your IPAM, DNS, and network segmentation strategies account for exponential traffic growth and non-human user proliferation before they outpace governance capacity.
Revisit NIST and European Standards for DNS Governance	Updated NIST standards for DNS security in the age of AI have been published and provide a strong governance baseline. Reviewing these frameworks does not require deep technical expertise — the fundamentals they codify are accessible to any leader willing to engage. If you have not assessed your posture against them, commission that assessment now.

Measure Detection and Recovery Speed, Not Just Absence of Incidents	If the foundational layer fails — whether through misconfiguration, a supply chain compromise, or a targeted attack — how fast can you detect, isolate, and recover? This metric is independent of whether an incident has occurred. Organizations that can answer it with evidence are resilient. Those that cannot are dependent on luck.

Time Stamps

TIME	CONTENT
0:00	Opening scenario — the October 2025 AWS global outage: $581 million in losses from a DNS misconfiguration
0:49	Host framing: the foundational infrastructure security blind spot — the governance gap beneath every other security investment
4:02	Scott Harrell welcome and introduction
4:18	Guest career highlights — Intel, Cisco (20 years, enterprise networking GM), Chapel Hill MBA, Infoblox President and CEO
5:20	Host and guest acknowledge their rival school affiliations — Duke, Georgia, UNC — and promise a congenial discussion
6:07	Unpacking the AWS incident: why it illustrates the brittleness of digital environments and the overestimation of cloud resilience
7:56	Why foundational infrastructure is overlooked: not technical failure — governance failure
8:37	The CrowdStrike lesson applied: boards that asked the right questions afterward identified DNS and DDI as Tier Zero services
11:45	Dr. Chatterjee explains DDI — DNS, DHCP, IPAM — for the audience: the naming, addressing, and inventory layer that connects everything
14:22	Making the case to leadership: how Harrell builds the governance argument for foundational infrastructure security investment
17:58	The CPD Framework applied to DNS governance — Commitment, Preparedness, Discipline — with leadership implications
20:48	Turning the network into a security sensor: 92% of malware leverages DNS; intercepting the first call-out prevents the cascade
24:33	Cross-episode reinforcement: Episode 105 guest Andre Robachevski on routing incidents — 200–300 per month, most invisible to security teams
26:16	Evaluation criteria for foundational infrastructure security: security-in-depth vs. security-in-kind; what differentiated coverage looks like
28:43	Preemptive vs. reactive security: tracking threat actor infrastructure before malware is weaponized; the dark-web link shortener example
31:05	The 95/5 spending imbalance: only 5% of enterprise security budgets allocated to preemptive activities; Gartner's 50/50 target by 2030
31:46	The litmus test: if a provider's work begins after malware has activated, it is reactive — regardless of how they describe their positioning
32:48	Dr. Chatterjee on the ROI challenge and the senior healthcare leader who admitted preferring to have experienced an attack first

35:10	Harrell's response: rolling the dice on reactive security in a world where incidents have ended businesses regardless of size or vertical
38:00	The agentic AI inflection point: 450x traffic per agent vs. human, exponential complexity, and the limits of classical detect-and-respond
41:54	Closing framework: three metrics every leader should demand — speed of deployment, proactive prevention rate, detection and recovery time
44:02	Additional closing takeaways: segmentation, NIST standards for the age of AI, and the imperative to change the reactive-to-preemptive ratio
46:29	Episode wrap-up and listener call to action

Memorable Quotes

> *The cause was not a sophisticated cyber attack. It was a misconfiguration in the foundational layer that nobody was actively watching. The organization was large, resourced, and technically sophisticated. The blind spot was not technical — it was a governance decision that had never been made. That story is the frame for everything we are discussing today.*
>
> **— Dr. Dave Chatterjee**

> *Everything you do in the digital world depends on DNS. It is the oxygen. It is what every connection relies on. And because it has always worked — because it is invisible when it works — nobody governs it. Until it fails. And when it fails, everything built on top of it stops.*
>
> **— Scott Harrell, President and CEO, Infoblox**

> *The routing system is at the foundation of the internet, and yet because it is so foundational, it is below the radar. If something bad happens on the underlying routing fabric, it often manifests as some other type of incident — an outage, a performance degradation. By the time you get to the essence of the problem, the incident might already be gone, but the damage is done.*
>
> **— Andre Robachevski, Technical Director, Global Cyber Alliance (Episode 105)**

> *67% of organizations handle SAP security reactively. But this dynamic is universal: if your security program only moves when an audit fires — or when an incident occurs — your posture at the moment of the next breach is essentially zero. The signals were never being watched. The discipline was never there.*
>
> **— Dr. Dave Chatterjee**

> *You might be able to respond in time. You might be able to fix it. But you're rolling the dice. And to your point — I have seen businesses be taken under or massively impacted by these events, regardless of size, regardless of vertical. And a lot of times, what is saddening is the same pattern repeats itself. You talk to people proactively. You tell them the stories. And until it happens to them, many of them do not think differently.*
>
> **— Scott Harrell, President and CEO, Infoblox**

> *Unless you make security intrinsic to your value proposition — unless the security strategy and the overall organizational strategy are aligned — in the long run, it could hurt the company. I have numerous stories where companies have called it a day, filed for bankruptcy, because they were not security conscious. This is not something you do when you have the time, or when the revenue goes up. That is not how security works.*
>
> **— Dr. Dave Chatterjee**

Dr. Dave Chatterjee | dchatte.com | dchatte@gmail.com | linkedin.com/in/dchatte