Q&A WITH BRIAN NEELY, CIO & CISO OF AMERICAN SYSTEMS

AMERICAN SYSTEMS

hackerone

The only constant in life is change. That statement couldn't be more true in the world of cybersecurity, and no one knows that better than AMERICAN SYSTEMS CIO and CISO Brian Neely. He has over 23 years of experience in information technology.

As a defense contractor, AMERICAN SYSTEMS provides IT and engineering solutions for complex national priority programs. In other words, they provide the infrastructure for national security initiatives for the U.S. government.

As you can imagine, the sensitive programs and data they hold makes them heavily targeted by sophisticated, determined, highly resourced nation-state threat actors. These aren't part-time criminals. Attacking defense contractors is their day job. Losing data would mean losing a competitive advantage on the battlefield. In short, lives could be at stake. That's not your average security breach, and their approach to security reflects that.

We sat down with Brian to learn a bit more about how he's seen the industry evolve, what's next and how hacker-powered security fits into the matrix.

Q: How has your role evolved overtime?

A: I began working for AMERICAN SYSTEMS in 1996 and spent the first 10 years of my career at AMERICAN SYSTEMS directly supporting the Army, Navy, and Intel communities. Today, my team and I oversee all IT systems, services, data, security and compliance for the enterprise. In the last few years, we've seen a significant shift towards security and compliance.

Brian Neely
Security Operations Engineer

Q: How does hacker-powered security fit into your larger cybersecurity strategy?

A: We regularly run security assessments by large firms like Mandiant, Optiv and Baker Tilly, these include internal and external penetration tests, red-teaming, compromise and forensics testing, insider threat assessments, table-top exercises, and even quality, process and regulatory compliance audits. We know how important it is to augment internal security with trusted partners, not only to provide assurance, but to also enhance our overall security posture. Recently, our HackerOne Challenge became part of our portfolio of third party, independent audits and gave us access to talent that AMERICAN SYSTEMS would not be able to obtain or retain full time. The carefully selected, diverse population of HackerOne Clear researchers applied their specialized and unique skills to give us a controlled approach to the crowdsourced security testing model. We moved from a traditional checklist approach to compliance,

to a performance-based, bounty-driven approach. Activating more than 100 different skilled hackers looking for high-risk vulnerabilities was extremely beneficial. Needless to say, HackerOne exceeded my expectations. We look forward to adding the crowdsourced security model to our portfolio of third party assessments moving forward.

Q: Hiring top cybersecurity talent is a challenge for all organizations right now. How has the skills shortage impacted AMERICAN SYSTEMS' cybersecurity efforts?

A: We've been very lucky to be able to hold onto key cybersecurity talent, with a great senior leadership team in place that averages well over a decade on my team. Even though we operate globally, our base of operations is in the Washington DC area. Talent acquisition and retention is exceptionally challenging in DC. It's an extremely competitive market amongst defense contractors, with most having very large practices focused on cyber for internal security and services sold to the U.S. government. Add to that, centers of security excellence like Langley, Quantico and the Pentagon, and now with large commercial entities like Amazon and Sony establishing security centers in the area, it is only becoming more competitive. At AMERICAN SYSTEMS, we like to keep a dedicated core team for CyberOps, a team of skilled security analysts and security engineers, and then augment the rest with MSSP providers and independent specialists like those on the HackerOne platform.

Q: Any other pleasant surprises? What benefits have you seen from working with hackers that you didn't expect?

LS: It was surprisingly easy to engage, setup objectives, develop a bounty structure, and execute the program from the start on the HackerOne platform. AMERICAN SYSTEMS also leveraged HackerOne's triage services to augment the work of our internal team. We built trust with the triage team in a short period of time, had full visibility throughout the engagement, and were pleasantly surprised by the variety of fresh perspectives from the hacker community on HackerOne. We also spoke to key staff from the Department of Defense that were instrumental in the "Hack the Pentagon" program who lauded the bounty-based program for all of the benefits that it provided.

Q: The cybersecurity industry is constantly changing, especially with new legislation, regulation requirements, etc. being introduced almost daily. How do you think the industry will evolve in the years ahead?

A: The value of data keeps going up, so threats keep expanding and evolving. We live in an information society. Protecting information is critical to our industry, and our Nation's security. I only anticipate more regulation and more auditing in the years to come, which is a good thing. While it sounds painful, I firmly believe that the defense industry needs to elevate its cyber posture to match the tenacity of its adversaries, and more formal regulation and maturity may be the only way to do it. What's more important than protecting the Country, its infrastructure and its citizens?

—

To learn more about HackerOne Challenges, visit https://www.hackerone.com/product/challenge.

HackerOne Has Vetted Hackers for Hundreds of Organizations Including:

GM · Starbucks · Lufthansa · European Commission · Twitter · Spotify · Hack the U.S. Air Force · airbnb · UBER · LendingClub · Hack the Army · Google Play · New Relic · Nintendo · Adobe · HBO · Dropbox · Snapchat · YAHOO! · PayPal · shopify · slack · yelp · verizon media · TOYOTA

With Over 1,400 Organizations, More Companies Trust HackerOne Than Any Other Vendor

CONTACT US