ANTHONY SIRAVO

CISO
LIFESPAN

U.S. HEADQUARTERS: Providence, RI

EMPLOYEES: 16,000+

REVENUE: $2.3 Billion

Since Anthony Siravo was last featured in our Profiles in Confidence in 2017, his role and responsibilities have evolved, along with his approach to addressing unprecedented challenges.

Siravo's IT security department has grown in size, with the addition of specific infrastructure team responsibilities, enabling significant growth in their security engineering capabilities. The new team added key functions such as web filtering, application whitelisting, network access control and mobile device management. Siravo explains, "The traditional security team wasn't necessarily a 24/7 shop in terms of being on around the clock to hop on a call at any time if needed. But now with network access control and application whitelisting, we're truly required to be in-line with the way our customers do business. And we are a 24/7 hospital system."

RANSOMWARE AND IoMT

Siravo has two key top priorities - addressing an influx of ransomware hitting their partners & affiliates and focusing on his IoMT (Internet of Medical Things) cyber protection program.

There has been a significant uptick in ransomware hitting their partners and affiliates which concerns Siravo from a security perspective for many reasons, especially since Lifespan is linked to them via VPN. To combat these persistent threats during partner outbreaks, the security team has cut VPN connections between sites, blocked emails and kept ransomware runbooks uptodate. Siravo feels his team has become faster at responding to affiliate ransomware threats in both a timely and appropriate manner.

He comments, "We're embedding testing into all of our controls on a monthly basis. It's a huge undertaking to find out what our weaknesses are for all this ransomware, which has a lot of variance. We're starting with the newest and working our way back. Tactically we are working on stopping what's called LOLBINS (Living off the Land Binaries) from executing maliciously in our environment. LOLBINS are actual legitimate files that are installed on your system by default and required by things like your operating system. When you install Windows 10 on your system, these files are installed and necessary for most normal operations. They're legitimate programs that need to run but the problem is all the new ransomware threat actors are taking advantage of LOLBINS."

These types of ransomware threats have garnered Board and executive interest who engage with Siravo and his team to discuss their approach and progress, along with any questions they may have. He says, "I've been giving more presentations and done more reporting to the Board.

They have a lot of the metrics that I report to my different information security governance committees. We now report out to them as well. Because things are getting closer to home, there have been some organizational changes and overall more interest from the executives, which obviously helps me get funding and support."

Siravo's second priority around the IoMT cyber protection program is a challenge due to strict FDA regulations, vendor security ignorance and the legacy nature of medical devices. These devices include things such as infusion pumps and x-ray machines that are not managed by the information systems teams in any way, and Siravo's security team has limited or no access to them. Many times, operating systems and applications may be out of date with legacy technology and vulnerabilities, posing a challenge for Siravo and his team to secure them.

He explains "As an example, an infusion pump has Telnet open, which is an insecure, clear text protocol. It doesn't even need Telnet to run, but these things are so antiquated and non-secure that they're not hardened. We must make sure that unnecessary and potentially vulnerable ports and services can't communicate from a network level, so nothing can be taken advantage of from that standpoint. That's a huge undertaking because we have to call up these vendors and say, hey, we know you're not going to work on security, but can you tell us what ports you actually need? What does this thing actually need to do to communicate? We're going to secure around it, we're not going to break any functionality of your device. We're not going to break the FDA regulations. We're going to go from a network level and not touch your device, but we're going to secure it to the best of our abilities."

REMOTE WORKFORCE IMPACT

Aside from budgetary and resource-driven restraints caused by COVID, Siravo says addressing the shift to a remote workforce has been a significant challenge and undertaking to address. The information systems team was required to create a more robust remote infrastructure that allowed additional VPN and Citrix connections which the security team now must apply controls to. Furthermore, his team continues to spend time educating the workforce on how to use remote technologies, Multi-Factor Authentication, and navigate programs they might have not used before.

From a leadership perspective, Siravo has shifted his approach to ensure he continues to boost morale and communicate effectively. He explains, "Previously, I'd pop in my team's offices on a daily basis. Obviously, I can't do that anymore. Before, I always knew what was going on and what people were working on by seeing them in-person. So now with COVID, I can't do that. Typically, security and IT people don't like video chat. My leadership style has shifted to a lot more items being tracked in a more formal written format via Kanban SaaS type applications versus verbal. That's how I keep track of what everyone's doing and have updates that way."

HYBRID APPROACH TO ZERO TRUST

Siravo says for most healthcare organizations, Zero Trust is not 100% achievable. His approach to Zero Trust is hybrid due to the complex nature of the healthcare industry inundated with legacy systems and applications, and complexities around the Internet of Medical Things. He comments, "It doesn't matter if you're behind the firewall, you don't trust that network. So that's how we're defining Zero Trust. Our approach here in healthcare, and probably other sectors as well, is a hybrid approach because for healthcare, we're required to use systems, applications and devices that don't support even basic antivirus, never mind advanced security tools. No matter what, we need a hybrid approach because we won't be able to do host-based Zero Trust security on these devices since we're not even allowed to install security tools on them."

He continues, "For the IS managed devices, including things the information system team manages and my team secures, all of our endpoint controls work on-premise the same way when you're off-premise. For example, when you're here on-site at Lifespan we may have Dropbox blocked, and when you pick-up your laptop and bring it home, Dropbox will also be blocked at your house. We have the same malware protection checking every URL link and file, advanced persistent threat detection, everything. It works the same way because all of the security we're setting up is host-based. It doesn't matter how bad that network is, it's the same rules applied. However, for the non IS-managed devices, we have to mitigate those threats as much as possible. These systems are not going home. They're all on our Lifespan production network but have no controls on them. There's nothing we can install on them. They can't really be Zero Trust because they're on that network. There's nothing we can do to them from a host-based security perspective, so we have to utilize network based protection to the best extent possible."