JERRY GALVIN

AVP SECURITY
NORTHWELL HEALTH

HEADQUARTERS: New Hyde Park, New York

EMPLOYEES: 76,000+

REVENUE: $13.4 Billion

Jerry Galvin began his career in defense, then worked in the entertainment industry for eight years before going into healthcare in 2006. In 2006, Galvin joined Northwell Health, New York State's largest healthcare provider and private employer. Northwell is home to 23 hospitals and more than 800 outpatient facilities, as well as the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell, The Feinstein Institute for Medical Research, urgent care centers, kidney dialysis centers, acute inpatient rehabilitation, sub-acute rehabilitation and skilled-nursing facilities, a home care network, a hospice network, and other services.

Galvin was the fifth member of the IT Security team back in 2007 and over the years witnessed the team grow to 80 people today. He has helped mature and strengthen the cybersecurity program and currently oversees Operations, Engineering, Identity and Access Management, Mergers and Acquisitions, and Project Management with about 40 people on his respective team.

> *"...we have seen the cybersecurity theater change greatly in the last six years. The whole theory of ransomware, phishing, drive-by downloads, insider threats, and more, has raised the roof of cybersecurity ."*

With a rich history of experience in security, Galvin says one of the biggest changes is threats. He explains, "Back in the 90s, you would just worry about Backups and Antivirus in case a virus came in the door or a drive failed. Even as far back as the 2010s, that was still very much the case. However, we have seen the cybersecurity theater change greatly in the last six years. The whole theory of ransomware, phishing, drive-by downloads, insider threats, and more, has raised the roof of cybersecurity ."

THE ABCs OF STRONG SECURITY

Galvin says that IT security is as easy as ABC. 'A' stands for 'all systems go' meaning they do everything in their power so none of the systems are down because of a cyber threat. 'B' is always 'be secure' and focusing on secure solutions and secure technology investments. Northwell is the largest private employer in the state of New York, so focusing 'C' on 'customer service' means keeping patients and employees secure and happy.

He continues, "As far as strategic priorities, the perimeter has changed. We can no longer secure just the enterprise. You basically built this fortress so that nobody could get in and you were secure about who could get out. And now your model has

> *"As the organization grows and the technology grows, the ability to protect also grows. And we always say this is such a huge organization that if you were to buy a $1 pencil for every employee, you are looking at $75,000 and that's just employees."*

changed because COVID came along and said, hey, we need people that will be able to work from home and not just for a snow day. And we need patients to be seen from home, not just come into a doctor's office, not just coming to a hospital. So you really had to open up those restrictions to support that ease and still keep it secure."

One of their biggest strategies is segmentation. Galvin explains, "The whole idea of everything being up to date to the latest vulnerability standard is very hard when you're dealing with historical systems and data, and all the technology that floats within any enterprise (printers, mobile devices, IP cameras, etc.). And then understanding IoMT where you are able to classify what a medical device is in the environment. What is the standard operation that it should have. When can you sense that something has gone wrong, whether it's under attack, whether it's data leaking, or the usage is three times what you normally see. So all these things are happening on a day-to-day basis in real time. And we want to make sure we stay ahead of any risks that arise."

TACKLING CHALLENGES

In most healthcare organizations, including Northwell, the standard project process could take months or sometimes years because of the large scale of work involved. However, many of the COVID solutions at Northwell were implemented in one week or month because they had to move fast to stay ahead of the waves of patients coming through their doors.

Budget is another challenge as healthcare dollars get harder and harder to earn, which Galvin says means they become harder to spend. He says they have been embracing multi-year deals or enterprise agreements to better maintain their overall spend. He comments, "As the organization grows and the technology grows, the ability to protect also grows. And we always say this is such a huge organization that if you were to buy a $1 pencil for every employee, you are looking at $75,000 and that's just employees. We still have a lot of people on top of that, vendors and consultants and community physicians. So at any given time, we're trying to keep tabs on a hundred thousand people."

"But the only other challenge has always been any time we are making a pitch about a trend or a direction, sometimes you come to the table and the first time you are there, people are looking at you like this is a little crazy, why do we need to do this? And then by year two, when you are coming back to that table, they say yes, some people are doing it, but we are not ready yet. And then by year three, it is what, this is not done yet? We have been lucky enough to always be one step ahead of the next cyber attack wave. We made a decision in the fall of 2019 to select and deploy an EDR solution and we got it out to 70,000 endpoints over a five-month period. Then March 2020 comes and that is when everybody went home because of COVID-19. That EDR was the one tool that protected those laptops and people's homesteads the most," explains Galvin.

IDENTITY

"At Northwell, we look to identify everything from the user, to the device, to the application, to the data, to the location, to the timeframe. And there are probably a few more scenarios, but you really need to wrap your hands around every little piece of it because each one can give you intel. Obviously for years, people just monitored the user. Now, we can monitor if an endpoint is usually generating one gig of data a day, why did it generate 10 gigs on a Saturday. Or the location, this device is usually coming from site X, why is it now coming from another site? And even the timeframe, when you look at network detect and respond, I think the theory of just monitoring somebody for what they are doing today has now expanded to what have they done over the last seven, or the last 30, or the last 90 days? You just get bigger and bigger with your threat model so you can pick up the smallest risk," explains Galvin.

He continues, "In terms of challenges, I think for us as it becomes more and more standard in the environment, it's being asked to do everything and not all systems are there yet to support it. You have many different theories of what identity is to each vendor. We have one application where not only is the user controlled for what they can see and what they can do, but the device that they do it from is controlled for what they can see and what they can do. When you change that model, you're taking a level of that security and removing it. So, it becomes a higher risk. And then when you take somebody and say you are working remote, it makes it an even higher risk. There's always an ebb and flow of we're going to support this for the time being, but we're going to bring it back to a more secure model as soon as we can." Basically, Dr. No is Dr. Go, meaning if you just keep saying no, the customer will look to someone else to say yes. So, we do our best to be Dr. How. How can we make this work. How can we do it securely. And so far, that's been working for 15 years!"