PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

KATHY HUGHES
CISO, NORTHWELL HEALTH

HEADQUARTERS: Great Neck, NY

EMPLOYEES: 61,000

ANNUAL REVENUE: $7.4 Bliion

AT THE HELM OF EMERGING DEPARTMENTS

Kathy Hughes began her career in manufacturing as a financial analyst, but she quickly transitioned to the computer and technology field, which was in its infancy. A business major with minors in computer information systems and economics in college, she was one of the few people well-versed in computer technology before most knew what computers were. She established centralized computing centers, installed computer networks and implemented distributed computing technologies. More recently, her career path has evolved to information security, where today she is CISO at Northwell Health, a healthcare network based out of New York.

As she developed in her career, she worked for industries as diverse as government contractors, publishing and retail. The one common thread across each job was being consistently tasked with developing programs to respond to changing business demands. "I like the challenge of establishing programs from scratch or bringing them to the next level of maturity by creating efficiencies which bring value and benefit to the organization. I also enjoy challenging the status quo, motivating staff to think outside the box and empowering them to drive change," said Hughes.

While working at a government contractor, Hughes created and managed the first Information Center, a shared computer center for company employees. From there, she took on positions of increasing responsibility, creating infrastructure services departments at other companies. A position as a outsource service provider for Northwell Health overseeing the Infrastructure teams, led to an opportunity to create and manage Northwell's

> "I like the challenge of establishing programs from scratch or bringing them to the next level of maturity by creating efficiencies which bring value and benefit to the organization."

disaster recovery program which gave her exposure to risk management. With the disaster recovery program well-established, the CTO of Northwell Health asked Hughes to take on the role of interim Director of IT Security, a position that lasted three years. Once a new Director of IT Security came on board, Hughes transitioned again, this time to develop a new, formal program for risk management. "In developing the risk management program, I was able to develop strong relationships with the Chief Compliance Officer (CCO) and Chief Internal Audit Officer (CIAO) which established a level of credibility when I transitioned to the CISO position," said Hughes.

BAPTISM BY FIRE

Northwell Health's CIO knew Hughes was the right person for the CISO position. Hughes acknowledges that her background in infrastructure, disaster recovery and business continuity, ability to successfully build programs, and the strength of her relationships with the CCO and CIAO, led to the CIO entrusting her with the increasingly important CISO position.

"I transitioned to CISO just as security was really becoming critical to healthcare organizations. As an industry, we have transitioned from paper to electronic medical records over the past few years, which has made us a prime target for cybercrime. This reality became a baptism by fire for me as well as for other healthcare CISOs."

"Really quickly in my tenure, we had some difficult incidents come up," continued Hughes. "I realized we needed to further enhance our programs. My team and I have worked very hard over the past year and a half to mature our programs, with adjustments to our organization, structure, budget and with senior leadership support. I communicated the program changes to senior executives at Northwell and helped them understand the environment and the threats. Other CISOs have had a bigger struggle than I have in that regard."

Hughes takes a plain language approach to communicating with senior executives. "Most people are very intimidated by security," said Hughes. "They know security is something they have to do, but the return on investment is difficult to calculate so it can be hard to justify. One session at a conference helped me put this into perspective. The speaker's advice was to relay complex security concepts into words that people can relate to. The best way to do that is through stories. Tell them a story of what happened at an organization like our own, what lessons were learned and how some of those lessons can be applied to our environment. When you explain security through stories, people can relate and quickly understand the very real risks involved. It helps people understand the business impact and get support for our initiatives."

TECHNOLOGY IS CHANGING THE HEALTHCARE INDUSTRY

At Northwell, similar to other healthcare organizations, the focus weighs heavily on creating innovative solutions to improve the delivery of healthcare services. For example, the company's Telestroke service allows doctors who may be offsite, to immediately respond and care for stroke patients. A timely response is especially important when dealing with stroke victims, enabling the Telestroke solution to save lives. Protecting the secure delivery of patient data from the hospital to the remote doctor is an important part of the process.

Northwell built an Innovation Lab, where vendors like Philips, Allscripts or GE may co-develop wireless or mobile tech solutions in a health environment without impacting patient care. "As the security team, we need to make sure we are involved from the beginning, and not viewed as an impediment to fast progress," said Hughes. "We need to enable innovation in a secure environment that is as transparent as possible."

According to Hughes, "While we have state-of-the-art security technologies in place supported by people and process, healthcare as an industry is playing defense and continually preparing for a security incident. We need to make sure we have a good response plan in place, if something does come up. We need to be prepared to respond with a tested process and already have in place alliances with outside entities like law enforcement, PR, media, cybersecurity firms, and forensic firms. We need to have the whole infrastructure of a response plan laid out, regularly tested and ready for different scenarios."

In some regards, Hughes believes the healthcare industry is lagging other industries, primarily due to recent government incentive programs to shift from paper to electronic medical records. As a result, Hughes looks outside of the industry when hiring. "I specifically look to onboard employees from financial services and retail because those industries lead in cybersecurity. They have faced more incidents and have more mature processes in place which can be applied to healthcare. I tell my employees you are protecting data in the same way, but in healthcare the responsibility is even more critical. When it comes to things like medical device and application security, you are literally protecting people's lives."