KATHY HUGHES

CISO & VP, NORTHWELL HEALTH

HEADQUARTERS: New Hyde Park, New York

EMPLOYEES: 68,000+

REVENUE: $12.5 Billion

Kathy Hughes was previously featured in a 2016 issue of Feats of Strength magazine. Today, Hughes shares her professional and team growth as it relates to strengthening the security program, continuing to ensure business goals are met and that Northwell Health is kept secure.

Hughes says the Information Security department has grown significantly over the past few years, with a heavy investment in awareness training and education, a strong focus on technologies and processes and steady progress within her team's roles and responsibilities. She comments, "At a very high level, my career has really been evolving based on the way the industry, and the needs placed upon CISOs, has been changing. We've had to look at how we're organized and how we're investing on a continuous basis to make sure we keep pace and adjust our processes and procedures. We've also had to change the way we work and interact with our staff, employees, business associates and patients, to make sure that we're doing it in the most effective, safe and efficient way."

She continues to focus on relationship building and relationship management to ensure the rest of the organization is aware and informed about security issues, threats, opportunities, challenges or gaps that might affect the security program. Hughes explains, "I'm on several committees where I have a seat at the table. Although it's virtual now, I get the opportunity to provide status on our security program to our senior management. My boss also provides an annual update to our Board of Trustees and quarterly updates at the Executive Audit and Compliance Board meetings."

The best way for Hughes to keep her business peers informed is through formal committees and meetings. She sits on the IT Risk Governance, Privacy and Security, Executive Audit and Compliance and PHI committees. Through these different committees, she communicates with her peers outside of Information Services and keeps them informed about what her team is working on, industry trends and where continued investments in people, process and technology are needed.

SOLID SECURITY FOUNDATION & COVID

"Expanding the remote workforce, making sure our research data was being protected and turning the knob up on monitoring those particular areas were things we had not planned to focus on prior to January. We also needed to expand protection on our internet connections, which required capacity upgrades as a result of the expanded workforce for intrusion prevention and for detecting potential DDoS attacks. We had all those foundational pieces in place, but the expanded use of these services literally

happened unexpectedly overnight. That forced us to reevaluate the investments that we had planned for this year and shift priorities to make sure we could meet more current requirements the business was saying that they needed us to support."

Fortunately, Northwell Health had a solid foundation in place around remote workforce processes and technology, so when remote work became mandatory, the organization was prepared. Hughes explains, "We just had to turn the knob up because there were some adjustments that had to be made, some additional capacity that had to be purchased, but we had a really solid foundation that we had to just expand upon. We also had to educate people who weren't familiar with how to access that environment. This was one of our biggest challenges, not only for Northwell, but for every organization that had to contend with an overnight expanded remote workforce. We were very well prepared for this and were able to very successfully execute in a short period of time."

She continues, "The second issue that we had to deal with was that instead of people accessing our network through office connections to data centers and cloud services, they were now accessing those same resources, through their home internet connections. So we had to expand other types of infrastructure, like our intrusion prevention system and our DDoS protection services, as examples, to coincide with the shift of the traffic from the internal network to the exterior."

Northwell's healthcare network includes research organizations, so Hughes and her team had to intently examine how to protect critical research data. They focused on ensuring anomalous behavior was closely observed, with help from local FBI Outreach resources who provided guidance, advice and suggestions.

FOCUS ON OUTPACING ADVERSARIES

Top of mind for Hughes and her team is consistently keeping pace or outpacing adversaries, and doing so in a forward-thinking, automated and comprehensive manner. One of the most important approaches her team is taking is understanding adversarial techniques and tactics for infiltrating systems, whether through social engineering or technical malware-type methods. They are focusing on threat management and threat intelligence to understand how these threats might potentially impact Northwell Health's systems.

Hughes comments, "The areas of artificial intelligence and machine learning, as it relates to not only threat detection, but also threat response, are key focus areas for us that we've continued to invest in. For example, if there's a zero day vulnerability that is identified and an IP address known to be exploiting the vulnerability, we want to make sure the IP address is blocked quickly. We do this by either manually blocking that particular IP address or by using our security technologies to automatically detect and block anomalous activity."

She continues, "We've been focusing on automation and behavior analytics solutions that put some of the work that normally or historically would have been done by people, into software that can now do it better, quicker, faster and more efficiently. Otherwise, people would be reading through billions of meaningless events and trying to pick out those that might indicate an incident requiring further investigation. Our strategy is to automate and leverage technology to the extent we can, and where it makes sense, instead of hiring additional people to parse through logs, so the staff can focus on the more critical tasks."

ZERO TRUST: PROCESS, APPROACH AND METHODOLOGY

To Hughes, Zero Trust is a process, approach and methodology - not a product or technology solution. She defines Zero Trust by never trusting and always verifying that someone is who they say they are.

She explains, "When you look back, even as recently as last year, people typically would work from a particular physical location. They go to an office building and in our case, they'd go to hospitals or physician practice sites. They would typically sign in from the same device, whether it's a laptop or workstation, to access systems and data. Now, the concept of Zero Trust has really gained momentum because that dynamic has changed significantly. Previously it was a buzzword, but now it's something that people really need to start paying attention to because working from a physical location from one device is no longer the norm. Now people are working from multiple locations, including home, and they're accessing systems from multiple devices. It could be their home computer, a mobile device or a kiosk device that they're accessing from a cafe. It's not always the same device. So this has introduced a number of challenges because the concept of securing an office building and making sure that you have firewalls to protect your perimeter has become an outdated concept."

To address Zero Trust, Hughes recommends having a process that includes different principles. She comments, "Zero Trust programs require Identity and Access Management solutions, an Asset Management system and a Multifactor Authentication system. It also requires making sure you have the appropriate technologies in place to segment the network which can be done statically or dynamically. It's making sure that users, based on least privilege and need to know, have access to only what they need and what they should have access to, and only the privileges that they need to carry out their job functions. If somebody does get onto your network who isn't authorized, you must be able to contain them by limiting what they can do and where they can go."