PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

PHIL CURRAN

Chief Information Assurance and Privacy Officer
Cooper University Health Care

Phil's Key to Success

"I surround myself with smart people. Our team is constantly looking at the way we are working and if we can do it better. We meet with business leaders all the time, and we are constantly assessing how we can provide more value to them and be more valuable to the business."

"IT'S NOT IF, BUT WHEN"

Recently, Phil Curran the Chief Information Assurance and Privacy Officer at Cooper University Health Care, was making his usual rounds when he ran into the CFO of the hospital. The CFO said, "I remember Phil - it's not if, but when." The quick exchange was positive proof that other senior leaders at the hospital were hearing and abiding by Phil's message of constant vigilance and preparedness when it comes to privacy and information assurance. "They (the board) are embracing information assurance as a strategic imperative," says Phil.

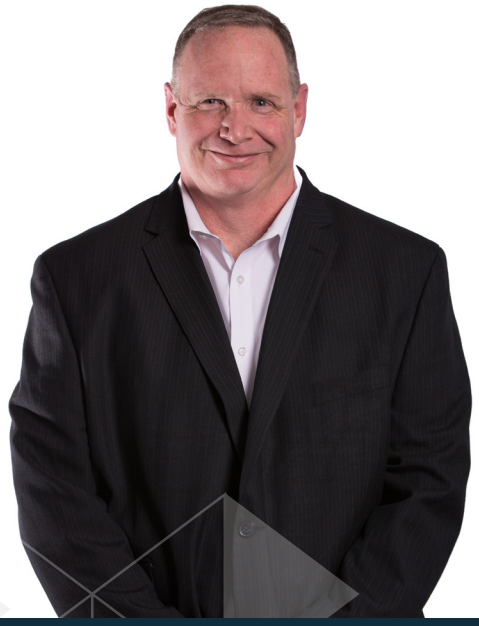
As a member of the hospital's audit committee, Phil has the ear of the Board of Directors on a quarterly basis. While major hacks and threats in the news may pique interest or spur specific questions from the board, Phil keeps them focused on ongoing information security awareness and preparedness by reminding them that "it's not if, but when." Outside of the Boardroom, Phil believes that face-to-face interaction and old-fashioned networking are vital to keeping security at the top of mind amongst business leaders who are managing budgets and making important decisions that may have dramatic impact on patients. Phil makes it a point to get out of his office and meet with other business units across the hospital's eighty plus sites in formal and informal interactions.

Checking in with colleagues and asking about their work has a number of benefits. First, it allows Phil and his team to keep up-to-date on business projects that require a security risk assessment – anything that involves health information or PII - but it also allows him to work as a

peer, not an adversary, or "security ogre". Phil says, "Business leaders understand risk. Our job is to present the security risks to them, and let them make decisions after reviewing all the information." Because Phil and his team have made an impression (via the meetings and networking), business leaders recognize the importance of preparedness and vigilance. As a result, they appreciate the merit of the risk assessments and weigh the results accordingly.

AN ORGANIZATIONAL CHANGE MAKES A BIG IMPACT

It was not always so easy for the Information Assurance group to reach senior executives with their message and value. When Phil first joined Cooper University Health Care he reported to the CIO, a common organizational structure in hospitals. This meant that risk and security policy were delivered to business leaders through the lens of the technology organization. As a result, communication between the Information Assurance & Privacy Team and business units was limited. When the hospital made the decision to move Phil's team out of IT (they now are part of the Compliance department), the collaboration and direct interaction between Phil's team and other departments improved dramatically. "Because of that change, we communicate risk directly to business units. The move out of IT was among the biggest factors in the success of our information assurance and privacy program."



SEPARATION OF SECURITY POLICY AND IT

"My role is to establish the standards and controls from an information perspective to maintain the confidentiality, availability, and privacy of our data. I am not a CSO. I do not handle security operations. My team focuses exclusively on governance, and not the technology used to enforce security policy. It can cause concern when the team responsible for maintaining the privacy and security of information is also the team responsible for bringing technology into the organization."

Gartner Agrees:

Today, only 38% of CISOs are outside of the IT department, but in their report, "Determining Whether a CISO Should Report Outside of IT", Gartner emphasizes a need to move CISOs out from under the CIO in the near term.