HOW ITSM CAN IMPROVE THE SECURITY POSTURE AND REPORTING FOR HEALTHCARE ORGANIZATIONS

According to a recent study from MIT's Sloan School of Management, hospitals experience up to 70 percent of all ransomware attacks. They're an easy target for hackers, because when health records are held hostage hospitals have no choice but to pay the ransom. To refuse to pay the ransom could compromise care, expose personal health information, and see harsh penalties levied on the organization.

In a recent interview with Chris Cullen of Perspectium explained that the decentralized nature of most hospitals makes them vulnerable to cyber attacks. "In most hospitals, IT is siloed from the security team, and the security team is siloed from the privacy and compliance team. They don't always talk to each other."

Cullen said that in some hospitals, you will

see integration between IT and security to run simulations and testing. “While this gives insight into network-level security and hardware security it doesn’t show you what the users are doing. That’s the gap,” Cullen explained. “The privacy department will typically use a different tool to analyze user behavior on the network and look for things like duplicate logins, logins from different locations, multiple logins at the same time and be able to advise employees against the behavior in the future.”

Cullen helps healthcare providers understand how IT service management (ITSM) can solve the challenges of service and data integration using technology with processes that extend beyond application silos. Cullen said that ITSM enables IT security to replicate ITSM data, so they can have a real-time copy of the current IT infrastructure environment to run attack-simulation or other security tests against the most up-to-date information.

Luckily, once a healthcare provider introduces a privacy monitoring system and employees are aware they are being monitored, the number of incidents drops. That is good news, but still doesn’t provide a full picture of what is happening on a provider’s network. “The ability to integrate the patient privacy system data with the ITSM data and the network-level security data, offers a full picture of the network and the behavior of users on the network to run reporting and analytics about privacy and report out,” Cullen said.

This is particularly important because the Centers for Medicare & Medicaid Services (CMS) require healthcare providers to file an annual privacy impact assessment for review of their compliance with CMS regulations
An extensive redesign last year transformed the privacy impact assessment into a smart form that is unique to each healthcare provider system. “Last year, CMS gave healthcare providers the opportunity to review and correct their forms. Going forward, however, this won’t happen and it’s a strong argument for data integration and process integration,” he said. “With the required data readily available, healthcare providers can easily populate the smart form, and submit the private impact assessment in an automated fashion.”

Cullen said that ITSM can play an important role in helping healthcare providers ensure that the most up-to-date data is available for CMS reporting.