Intrinium Builds and Leads an IT Security Program to Keep Verity Health System Secure and Compliant

CHALLENGE

Verity Health System of California, formerly known as Daughters of Charity Health System, is a non-profit regional health system with four hospitals in Northern California, two in Southern California, and ancillary clinics, ambulatory surgery centers, and urgent care facilities across the state. The health system is dedicated to efficiently delivering quality healthcare to diverse patient populations while providing community benefits through various outreach programs and wellness activities.

After struggling financially from significant operating losses, the Daughters of Charity Health System Board of Directors selected BlueMountain Capital Management to revitalize operations and transition leadership to the new Verity Health System. At the time of this transition, each of the hospitals ran independently when it came to their security functions. The Board of Directors and the CIO determined that a centralized information security function was necessary for the long term protection of the System's security, patient data, and mission.

When the new Chief Information Officer (CIO) arrived, embarked on a mission to centralize IT functions, update the technology environment and implement a repeatable, mature information security controls structure within the organization.

SITUATION

In April 2016, Nolan Garrett of Intrinium became the interim CISO, and over the course of a couple of months, he brought in additional Intrinium staff to help build a reliable IT security program. The team became fully engaged in building and leading the information security program as well as providing supplementary support for projects as needed.

When the team first arrived, they found outdated infrastructure such as firewalls, network switches, endpoint computers, servers, and other data center equipment. Due to the financial struggles of the previous organization, this infrastructure had not been maintained to the standards one would expect in a modern healthcare environment.

SOLUTION

The Intrinium team built an information security program based on the NIST Cybersecurity Framework (CSF). They re-wrote all policies and procedures from a security perspective for the entire Verity system. The team evaluated all of Verity's processes including data management, new user access and permission control, and vendor contract management.

Then, the team performed a broad, full-scale penetration test and vulnerability assessment of all 6 hospitals, ancillary clinics, data centers, and corporate offices, which generated a substantial amount of issues that needed to be addressed.

Intrinium Builds and Leads an IT Security Program to Keep Verity Health System Secure and Compliant

SOLUTION (cont.)

After taking all the information they had gathered these assessments, the Intrinium team then started to build a remediation plan and multi-year roadmap to help Verity Health System get to where they needed to be from a IT security health perspective.

Historically, Verity had not evaluated risk from an enterprise perspective, so the team also performed full risk assessments for the entire Verity Health System, including its ancillary surgical centers. Intrinium became deeply integrated in building Verity's risk assessment process, which the health system could then use to drive budget allocation in order to get the best results for their investment.

RESULT

When Intrinium first arrived, they were able to address some immediate concerns. Verity Health System experienced two security incidents that occurred early on, but with the security team now engaged, they identified the threats and protected Verity from any long-term issues. Intrinium then put the policies, procedures, and technical tools in place to enable Verity to protect themselves in real-time.

When the May 2017 WannaCry attack and other ransomware outbreaks recently occurred, Verity did not experience any ransomware infections as the team was able to completely protect the environment from an outbreak. By leveraging the Intrinium Security Operation Center (SOC), the team was able to block all potential indicators of compromise and threat vectors that were occurring at Verity's perimeter. Then, they went through to protect the internal infrastructure as a secondary step. Since the team had implemented effective tools and leveraged Intrinium's SOC, they were able to stay ahead of the attack, leaving Verity with very little chance of compromise.

LONG-TERM BENEFITS ESULT

By building a secure and reliable information security framework that prevents incidences from occurring, Intrinium helped Verity Health System reduce costs of overall security management, especially incident response costs.

Intrinium also helped Verity avoid penalties and reduce costs related to regulatory issues from the OCR by building risk assessments that helped ensure that Verity is compliant with HIPAA standards.

Verity Health