



The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

YEAR:
2012

STATUS:
Laureate

Organization:
Lehigh Valley Health Network

Organization URL:
<http://www.lvhn.org/>

Project Name:
Lehigh Valley Health Network Patient Security Initiatives

What social/humanitarian issue was the project designed to address? What specific metrics did you use to measure the project's success?

The Lehigh Valley Health Network developed and implemented several large network security initiatives in response to protecting its patients and their sensitive personal data. Healthcare institutions such as LVHN are unique entities in that they store complete virtual identities of their patients, including medical, financial, and personal data. With the plethora of sensitive data and the potential for data breaches, LVHN developed a comprehensive road map to ensure their network's data remained secure, and thus the patient's identity and safety as well. Lehigh Valley Health Network measured the success of their project through extensive data testing, policy creations, and network monitoring. Once the policies were created to restrict sensitive data loss in the various implementations executed, LVHN Information Services Security personnel thoroughly tested the policies to reduce false positives and ensure that sensitive data was not leaving the network. With identity theft on the rise, the Lehigh Valley Health Network's widespread network security initiatives further protected their patient's data and further ensured the safety of the patient.

Please describe the technologies used and how those technologies were deployed in an innovative way. Also, please include any technical or other challenges that were overcome for the successful implementation of the project.

Members from LVHN's senior management and the I/S Security team adopted a phased approach with their security initiatives after careful analysis of where breaches occur most. Mobile device encryption was decided as the highest priority and was rolled out to 3,000 laptop devices within the year. In the event of a lost or stolen laptop, LVHN patients were now protected from an unauthorized attempt to gain their information stored on the devices. A second critical area of concern for LVHN was the data leaving the network via email. In only a few months, all of the network's corporate email was funneled through an encryption engine that automatically scanned for any sensitive data as defined by policies. This process protected LVHN patients by ensuring any confidential data was readable only by the intended recipient. A third major project to secure the data within LVHN was to analyze all data stored on over 7,000 desktop hard drives and move the sensitive data to a secure server location. All other data was then deleted from the local hard drives of the workstations and technical policies were enacted to prevent any further files from being saved to the local drives. The final chief security initiative for LVHN in 2011 was the adoption of a Data Loss Prevention system. DLP monitors all transmissions going outside of the LVHN network regardless of the protocol. LVHN once again relied on the careful adoption of tested policies to reduce false positives while ensuring business needs were met. The DLP system automatically blocks any unsecured sensitive data and notifies the end user of the policy that is being broken as well as steps to send the data securely. LVHN successfully adopted these initiatives while ensuring the critical business of the hospital wasn't interrupted.

Please list the specific humanitarian benefits the project has yielded so far.

With the Health Information Technology for Economic and Clinical Health Act (HITECH) signed into law, LVHN realized the need to continue their previous efforts to protect the patient's sensitive information. This realized need involved the network-wide adoption of mobile encryption, email encryption, hard drive lockdowns, and data loss prevention. The Information Services Security team understood the need for data transmission to occur to ensure critical business processes continue. With the implementation of automatic email encryption and the data loss prevention program, LVHN guaranteed the continuation of business processes through secure transmissions, while blocking any communications via unsecured means. Mobile encryption and hard drive lockdowns ensured the health network that no patient data would be recoverable from a stolen or missing hospital workstation. With identity theft on the rise and the vast amount of sensitive information stored within the hospital from a patient, the Lehigh Valley Health Network took great strides in closing the gap for potential data breaches and stolen identities of the network's patients.

Please provide the best example of how the project has benefited a specific individual, enterprise or organization. Feel free to include personal quotes from individuals who have directly benefited from the work.

Lehigh Valley Health Network has taken a firm resolution to ensure the protection of the patient and their sensitive data. While the safety of the patient can be measured in medical terms and prognosis, it can also be defined in terms of the security of the patient's sensitive data and protection from identity theft. Through the four core security measures LVHN has implemented in 2011, the patient is assured the safety of his or her personal information. This assurance complies with all federal regulations (HIPAA, HITECH, etc.) and helps LVHN fight the potential of a data breach from occurring. Increasingly companies are in the news for data breaches, fines, identity theft, and lack of oversight to protect their patients or customers. The Lehigh Valley Health Network has committed itself to the security of their patients and to ensuring no avenue of data loss is left unprotected.