BioSpectrum the business of Bio & Health Sciences ASIA EDITION

Healthcare information security, privacy will be priorities'

14 February 2014 | News | By BioSpectrum Bureau

Technology will continue to play a crucial role in improving the quality of healthcare delivery in 2014. Electronic health records (EHR) adoption will remain a key focus for health organizations to enable a more effective exchange of patient-relevant information between stakeholders. Despite varying levels of technology adoption and digitization in highly fragmented Asian regions, prevailing cloud, social media and BYOD trends will by and large improve the engagement between patients and healthcare providers. Along this transformation is a colossal amount of digital information that needs to be managed smartly and securely. Health Information at Risk The privacy and security of personal health information has become a globally recognized issue and priority.

According to the 2013 (ISC)2 Global Information Security Workforce Study, more than 12,000 respondents in the healthcare industry identified breach of laws and regulations as their top security priority. Security threats come from within and outside healthcare organizations. Security threats come from application vulnerabilities, malware, mobile devices, cloud-based services, internal employees, contractors, and hacker activities, to name a few.

Human error remains the leading cause of health information breaches. Ponemon Institute's December 2012 study, "Patient Privacy & Data Security" estimates that the average annual cost to the healthcare industry could potentially be as high as almost $7 billion. The Ponemon study also calculates that the average cost for the organizations represented in this benchmark study is $2.4 million over a two-year period." The Study also reveals that, "The top three causes for a data breach are: lost or stolen computing devices, employee mistakes, and third- party snafus."

While countries around the world have attempted to manage the issue and improve the effectiveness of security and privacy controls through numerous laws and best practice frameworks, little progress has been made in reducing the number of breaches. When combined with severe penalties agencies are now imposing including, heavy fines and sometimes criminal prosecution, the magnitude of risks borne by entities handling patient health information is resulting in even more diligent and vigorous efforts to protect the information. Critical guardians of informational assets There is a mounting need to ensure knowledgeable and credentialed security and privacy practitioners are in place to protect sensitive information. With that in mind, employers across the globe recognize the criticality of mitigating risk through improved hiring and training practices to ensure their security and privacy practitioners are qualified to do their jobs well. Until now, there has not been a credentialing program to validate a practitioner's core knowledge, skills, and qualifications to protect and keep secure vital healthcare information.

To address that (ISC)2, a global not-for-profit membership body of certified information and software security professionals worldwide, has developed a new certification, the HealthCare Information Security and Privacy Practitioner (HCISPP), to fill the gap between a simple awareness certification applicable to most healthcare workers, and by advanced professionals who have the depth and breadth of experience to qualify for senior-level positions.

Available worldwide, the HCISPP credential is aimed at providing healthcare employers and those in the industry with validation that a healthcare security and privacy practitioner has the core level of knowledge and expertise required by the industry to address specific security concerns.

The HCISPP credential is based on direct feedback from the (ISC)2 membership and industry luminaries from around the world working in healthcare who observed the evolving complexity of information risk management in the industry as online system migration and regulations have increased. At the Forefront of Healthcare Security & Privacy To attain the HCISPP certification, applicants must have a minimum of two years of experience in one knowledge area of the credential that includes security, compliance, and privacy.

Legal experience may be substituted for privacy. One of the two years of experience must be in the healthcare industry. All candidates must be able to demonstrate competencies in each of the following domains:
Healthcare Industry: Understand diversity of healthcare industry, types of technologies, flow of information, and levels of protection.
Regulatory Environment: Identify and under- stand relevant legal and regulatory requirements and ensure organization's policies and procedures are in compliance.
Privacy and Security in Healthcare: Basic understanding of security and privacy concepts and principles, types of information to protect.
Information Governance and Risk Manage- ment: How organizations manage information risk through security and privacy governance, risk management lifecycles, principle risk activities likely to support.
Information Risk Assessment: Understand risk assessment concepts, identify and participate in risk assessment practices and procedures.
Third Party Risk Management Identify third parties based on use of information, help manage third party relationships, determine when additional secu- rity and privacy assurances are required.

The HCISPP credential is a demonstration of knowledge by security and privacy practitioners regarding the proper controls to protect the privacy and security of sensitive patient health information as well as their commitment to the healthcare privacy foundation.

It is a foundational credential that reflects internation- ally accepted standards of practice for healthcare infor- mation security and privacy. For executives accountable for protecting sensitive healthcare data, HCISPP demon- strates a proactive commitment to ensure that an organi- zation is making the necessary human resources invest- ment for information security.

The HCISPP provides multiple benefits for healthcare security and privacy practitioners and the organizations that employ them. For practitioners, HCISPP:
Validates their experience, skills and competencies.
Demonstrates the qualifications to implement, manage and/or assess the appropriate security and privacy controls.

Enhances credibility as a healthcare information security and privacy practitioner. For organizations, HCISPP: Provides reinforced defense with qualified, experienced and credentialed healthcare information security and privacy practitioners.

Demonstrates the organization's proactive commitment to minimizing the risk of breaches.
Increases credibility of the organization when working with clients and vendors.