The Fifteenth National HIPAA Summit

Overview of Approaches
to
Security Officer Training

John Parmigiani
December 12, 2007

Fundamental Questions

- **What does a Chief Information Security Officer (CISO) or a ISO need to know to do his/her job effectively?**

- **How can he/she gain the necessary knowledge?**

How People Learn

- **Hearing (10%)**
- **Seeing (40%)**
- **Doing (50%)**

“Knowing is not enough; we must apply
Willing is not enough; we must do”
-Goethe-

“What I hear, I forget.
What I see, I remember.
What I do, I understand.”
- Confucius 451 BC-

Fundamental Attributes of an (C)ISO…

- **Not just technical, also administrative**
- **Manager, facilitator, coordinator, initiator**
- **Must understand the business processes and the data flows (usability vs. security: "know thyself")**
  - **What data (sensitive and non-sensitive) exists and in what applications**
  - **Where it begins, who touches it (internally and externally and user privileges), what is done to it, on what devices (mobile and stationary), when it is backed up**

Fundamental Attributes of a CISO…

- **Have knowledge of and be able to discuss with technical and administrative staff**
  - **Access controls**
    - **Authentication**
      - **Multi-factor (biometrics)**
    - **Authorization**
  - **Audit controls**
  - **Network protection**
  - **Data management and protection**
    - **Encryption**

Fundamental Attributes of a CISO…

- Security requirements in the SDLC
- Virtualization
- Disaster Recovery/Contingency Planning/Business Continuity …"93% of companies that suffer a significant data loss are out of business within five years" … US Bureau of Labor
- Policy/procedure development and implementation

- Be able to perform a risk analysis (vulnerabilities, threats, probabilities, impacts) , devise corrective action plans, formulate and administer risk management strategies

Fundamental Attributes of a CISO…

- **Develop, oversee, and participate in the delivery of security training, education, and awareness programs**
  - **In-house training (face-to-face, e-learning, contracted, organization staff)**
  - **Train-the-trainer**
  - **Special days, newsletters, log-on banners, posters, promotional products, screen savers**
  - **Intranet “security tips” page**
  - **Special presentations**

Don’t just tell them what to do, show them how!

Fundamental Attributes of a CISO…

- **Understand federal, state, local (and international, if necessary) regulatory requirements for data protection and enable the organization to be compliant**
- **Understand the nexus/convergence between physical and logical security controls**

Fundamental Attributes of a CISO

- **Be able to quickly respond to alleged security incidents in accordance with an established and tested process (work with HR, legal, IT, PR and law enforcement)**
- **Be able to measure the effectiveness of the organization's security program and report it to various levels (governance, administrative, and technical) of the organization**

Staying Effective as a CISO

- **Keep up with "best practices" not only in health care but also in other industries where sensitive data includes intellectual property, proprietary information, financial data**
- **Join professional organizations- CSI, SANS, etc.**
- **Attend conferences and technical training sessions on-line and in person; university training in information assurance, forensics, etc.**
- **Seek certification: CISSP, CISA, CISM, GIAC, etc.**

Conclusions

- **The CISO should be a well-informed, multi-faceted individual**
- **He should be immersed in a continuous effort to gain greater education and awareness and be dedicated to passing along relevant training to the organization with a goal of making good security practices second nature**
- **There are numerous opportunities available in today's multi-media environment for learning new techniques and approaches and keeping up with best practices**

Thank You !

Questions?

John C. Parmigiani
410-750-2497
jcparmigiani@comcast.net
www.johnparmigiani.com