Getting Security Right: The CISO of the Future

Presented by:
Mac McMillan
CEO, CynergisTek
Your Cheese Has Moved

Will You Be Immobilized, Or Adapt?
Security Challenges Have Increased

2014 has seen an increase in every measureable category of risk

- Insider threats
- Supply chain risks
- Medical device insecurity
- Malware & Advance Persistent Threats
- Mobile devices & mobile apps
- ID Theft & Fraud
- Physical theft & loss
- Emerging threats
We can’t afford not to embrace security

The Costs Of Security Have Increased

- Discovery, Notification & Response
- Civil Penalties
- Criminal Penalties
- VBP Payments Impacts
- Business Disruption
- Federal CAP/RA
- Insurance
- HCAPPS Score Impacts
- ID Theft Monitoring
- State Actions
- Degradation of Brand/Image
- Patient Confidence/Loyalty
- Investigation/Review
- Law Suit Defense
- Distraction of Staff
- Physician Alignment/Nurses and Staff Agreement

Insurance

- Medical/Malpractice
- Business
- Employee

Penalties

- Civil
- Criminal
- Civil/Federal
- Criminal/Federal

VBP

- Adjustments
- Revenue
- Capitation

Impacts

- Patient 
- Staff
- Field
- Leadership
2014: The Short List

Increases in every category

- **4M medical records** maintained on **four workstations**
- Physician loses laptop with psychiatric patients records
- Neurologic institute accidentally **emails** 10,000 patient records to 200 patients
- Phishing/hacking **nests nearly $3M** from six healthcare entities
- University reports laptop with patient information stolen out of a **student’s car**
- **Vendor** sells hospital’s X-rays (films) to third party
- Resident loses track of USB with over 500 orthopedic patients information
- **Portable electronic device** with patient data stolen from hospital
- 2200 physicians victims of **ID theft/tax fraud**
- Vendor sends **800 letters** with patient information to the wrong addresses.
- **Printers** returned to leasing company compromise thousands of patient records
- Health System reports third **stolen laptop** with 13,000 patient records
- 400 hospitals billings delayed as clearinghouse hit with **ransomware**
More than 90% of processes are automated, patient information is digitized and devices are networkable.

- Today’s CISO has to understand the needs of the business as well as have the security expertise to match the demands of both the threat and the business. Simply understanding HIPAA is not enough in today’s modern health IT environment. It’s not about compliance, it’s about assurance.
And Yet, We Still Suffer From Insufficient Resources

Adequate Security Requires Appropriate Investment

- In the 2014 HIMSS study HC CISOs gave themselves an average maturity rating of 4.35 on a scale of 1-7
- Many report missing critical technologies to fight today’s threats
- More than half of healthcare entities spend less than 3% of their IT budget on data protection
- Less than half have a full time CISO or information security manager
- Many healthcare security managers are first timers
Organizational Placement

The Recurring Debate
CISOs have been found in many different organizations within Healthcare entities. The majority are found in Information Technology, followed by Compliance, Finance, Legal, and occasionally a few others.
The Debate

90% of CISOs report to the CIO, but should they?

• **Pros**
  - Access to Executive leadership
  - “C” level skills and organizational awareness
  - Easier to make change in IT to promote security
  - Increases influence for CIO

• **Cons**
  - Information security oversight is limited
  - May detract CIO attention from other priorities
  - Conflicts of interest
  - Loss of full organizational focus
The short answer is that CISOs have been equally successful and not so successful in just about every organizational structure that exists. The keys to success or failure include the ability of the person, the level of visibility of the position and the amount of real support for the program, the position and the person. If the Board or the Executive team is not being briefed by the CISO on a regular basis in today’s environment they should be asking why.

“When the Board took an interest in the program, things changed, resources started coming.”
Core Security Skills
Experience, Education & Certifications
CISOs must be capable of leading security efforts

- **Security/Risk Management**
  Possess the knowledge and skill to develop and implement an integrated security and risk management program for the institution.

- **Security Governance**
  Facilitate security governance through establishing appropriate coordination and oversight activities and bodies.

- **Security Policy**
  Possess the writing and oratory skill to create and communicate polices and procedures needed.

- **Enterprise Architecture**
  Possess the ability to liaise with the enterprise architecture teams to ensure integration of security considerations.

- **Security Frameworks**
  Possess the ability to interpret, integrate and apply a unified security framework to address all laws, regulations, standards, etc. that apply.

- **Security Compliance**
  Ensure appropriate controls are implemented to meet or exceed compliance requirements.
Functional Skills

CISOs create the vision for security and drive change

- **Security Liaison**
  Lead the coordination of security issues across other key elements such as Compliance, Legal, Internal Audit, Compliance, etc.

- **External Coordination**
  Establish liaison with external agencies such as law enforcement to receive timely updates and maintain a strong program presents.

- **Measure Performance**
  Establish and report out regularly metrics that show program status, resource usage and increases in maturity.

- **Collaborate**
  Participate in committees with other disciplines to insure security is considered and implemented appropriately.

- **Security Vendors**
  Establish and report out regularly metrics that show program status, resource usage and increases in maturity.
Quality/Customer Service Skills

CISOs must insure the security program meets expectations

- **Vendor Security**
  Develop and implement processes to assess risks associated with external service providers, consultants and partners.

- **Governance**
  Contribute to governance activities and create a culture of program accountability to stakeholders.

- **System Selection**
  Implement procedures to insure timely acquisitions and mergers of information resources and facilities.

- **Communicate**
  Provide regular reporting on the status of the information security program to key stakeholders, and the Board.

- **Service Level Agreements**
  Use information security frameworks to guide program outcomes and service expectations for stakeholders.

- **Resource Planning**
  Implement budget and resource planning that solicits key stake holder inputs and priorities.
Safety/Risk Management Skills

CISOs must ensure security controls contribute to patient safety and provision of care priorities.

- **Business Continuity**
  - Establish disaster recovery and emergency operations plans in close coordination with business continuity program management objectives.

- **Security Incidents**
  - Implement proactive measures to identify, investigate, document, and communicate potential and real breaches.

- **Security Audits**
  - Conduct and assist in auditing security controls and processes to ensure effectiveness and integrity.

- **Risk Remediation**
  - Define and facilitate risk assessment efforts that inform risk remediation efforts on an ongoing basis.

- **Threat Awareness**
  - Proactively monitor external and internal threat environments and advise others on appropriate measures to mitigate risk.

- **Security Analysis**
  - Analyze information from incidents, logs, assessments, processes, workflows, etc. to identify to inform selection/implementation of controls.
Personal Skills
CISOs Must Master Soft Skills

- **Leadership**
  Real leadership comes through influence. The CISO needs to be able to set the vision and motivate the organization to follow.

- **Relationship Management**
  Building alliances is critical to success. Building rapport and understanding what is important, and providing support is how you get support.

- **Risk Management**
  Understanding risks to the business, not just systems and data, is critical to being relevant and heard.

- **Business Knowledge**
  Business leaders expect CISOs to be able to relate security requirements to the objectives of the business.

- **Strategic Planning**
  Planning is a critical business skill used to communication direction, priorities, objectives and the basis for measuring success.

- **Psychology/Sociology**
  The most dynamic component of security is human behavior. CISOs must understand individual and group behavior.
Selecting The Right Person

Important Considerations
Are Certifications Important?

Organizations need security leaders with both education and experience.

**Basic Learning**
Certain certifications represent a starting point in determining some formal knowledge of security principles and practices.

**Advanced Learning**
Other certifications demonstrate specialization in a particular security discipline or focus and depth of knowledge.

**The Right Certification**
When it comes to selecting a ISO certifications that demonstrate more practical knowledge of managing security like the CISM are more valuable, as are other certifications that show a broader experience like PMP, CHP or CISA.

**Most Important**
There is no replacement for experience which is far more important than certifications. Certifications say “they should know how to do it”, experience says “they have done it”.
Traits To Look Out For...

When Techie Meets CISO

- Technical challenge
- Concrete non-ambiguous solutions
- Task oriented
- Mastery of technical skill

- Hands-on training focus
- Documentation aversion
- High level of individual contribution
- Meetings are distractions
What To Look For
People Who Can Create Success

**Information**
People like to know what is happening and why. Provide updates often, synthesize essential points and deliver in concise messages.

**Alignment**
Look at security from the customers point of view, if you are perceived as understanding their plight/goals they are more apt to listen.

**Appropriateness**
Apply security realistically, keep it simple when possible, so when hard decisions are necessary they’ll be more supportive.

**Service**
Remember the business does not exist for security, security exists because of the business. Your job is to serve, to enable.
Today’s CISO Must...

Key Attributes of an Effective CISO

• Be a leader
• Possess business acumen
• Be comfortable managing risk
• Embrace enablement
• Think strategically, act tactically
• Be an effective communicator
• Be able to drive process
• Understand and apply psychology/sociology
• Be politically savvy, and
• Know privacy & security
• Possess endless curiosity
The CISO Of The Future

Questions?

Mac McMillan
mac.mcmillan@cynergistek.co
512.402.8555