Highly Credentialed Chief Information Security Officer (CISO) who defines and executes the technology direction, along with policies, governance, and standards, to protect highly sensitive data for risk-averse healthcare organizations. Broad and deep experience in all dimensions of cyber security and compliance. CISO-level presence and strategic leadership abilities well-suited to consulting with executive leadership about the strategy, vision, and direction of security, auditing, and regulatory compliance corporate initiatives.

Certifications

Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CISSP)
CompTIA Cybersecurity Analyst (CySA+)

Professional Experience

Company Name, City, State 2008 – Present
Information Security Officer

Building and maintaining an enterprise information security program for one of the nation's top pediatric healthcare systems, with 12,000 business users. Established and executed a security vision, with a sustainable technology roadmap, to shape a secure and reliable future. Manage direct enhancements to the system security architecture.

Security/Risk Assessments: Conducted comprehensive security assessments to manage vulnerability threats and prevent penetration. Quickly identified and eliminated gaps that put the organization at significant risk.

- Identified at-risk systems on the main campus and 60 offsite locations during a security assessment of a Windows workstation configuration. As a decisive decision maker, assumed responsibility for taking proactive measures to transition to a fully automated process.
- Collaborated with a consultant to analyze requirements and design an effective architecture.
- Delivered a no-cost solution that successfully pushed security patches and updates to any Windows device across the organization.

Security Management: Led projects to strengthen device security, improve control over user accounts, provision secure remote access, encrypt laptops, and deploy multifactor authentication.

- Worked closely with the medical community to develop a highly tailored, content filtering solution for email and websites; balanced risk against the community's need to access information. Remained highly responsive to any concerns.
- Led a security group to define enterprise requirements for a malware prevention solution. Researched and selected product and worked with IS staff to deploy a phased approach across 5,000+ PCs and servers.
- Established clear visibility into network traffic and potential attacks with an intrusion detection system, using behavior-based network protection with little impact on IS staff time or resources.

HIPAA Compliance Strategy: Forged a coalition with the Corporate Compliance Officer and the IS Manager regarding HIPAA Privacy to define and plan an implementation strategy.

- Held regular corporate meetings to educate executives on HIPAA regulations and present an approach for closing compliance gaps. Drove discussions with technical management to educate them on the significant risk of noncompliance. Developed training materials for all staff members to easily understand regulations.
- Established a solid policy framework, encompassing both information and HIPAA security, covered access and authorization, storage and media use, contingency planning, risk management, incident management, transmission security, and workstation security.
- Ensured solid footing for HIPAA security starting from day one.

HIPAA Compliance Projects: Ensured compliance and auditability with tightly controlled procedures.

- Proactively worked with the financial team to meet new regulations for eBilling transactions and to map electronic transactions to EDI-based standards.

- Built a high-performing security team and led numerous projects, including encryption, refinements in user provisioning, and assessment/modification of system security settings. Reviewed and modified server and workstation settings to meet regulations.

Disaster Recovery & Contingency Planning: Led effort to justify and implement enterprise contingency planning.

- Performed a Business Impact Analysis to identify critical resources and impacts to operations, patient care, and finances during system downtime. Identified risky procedures that prevented full backups.
- Defined vendor selection criteria and submitted an RFP to major disaster recovery providers. Selected best fit vendor to provide hot-site recovery services for all data center-based equipment and applications. Negotiated contract approved by senior management.
- Led a project to increase backup capability and speed based on implementation of SAN storage in combination with a robotic tape drive. Performed two successful recovery exercises, including network connectivity and application testing.

Electronic Medical Records: Applied persuasive communication skills to lead strategic planning meetings comprised of 15 security leads, project leadership, and an Internal Audit team; defined, designed, and built an integrated security plan for a $175M Epic system implementation.

- Reviewed and analyzed the roles and responsibilities of staff members to extend access to non-employees, such as physicians and affiliated medical staff, using role-based security—a more secure process, monitored against staff member's department and position.
- After go-live, the volume of security calls was far below the expected number, thereby demonstrating a very successful implementation.

Healthcare Organization 2001 – 2008

Director of Information Systems Audit

Directed an internal audit function for a $1B, multi-state healthcare system with 13,000 business users. In cooperation with the Director of IS, managed all enterprise-wide I.T. projects.

- Defined and executed audit strategies, including plans, policies, and programs, and monitored the effectiveness of the audit function.
- Led and continuously improved enterprise-wide information security, I.T. change control, and I.T. risk and compliance management programs. Collaborated with key stakeholders to prioritize security initiatives.
- Instituted an I.T. standards committee and corporate management reports.
- Created information security plans and policies. Developed the corporation's information security policy framework.

Education and Professional Development

Bachelor of Arts, English, University of California, San Francisco, 2000

Pacific Northwest Regional Leadership Forum, Society for Information Management, 2019
Southern California Regional Leadership Forum, Society for Information Security, 2015