Job Description

Job Title: Senior IT Security Specialist
Reports To: Director of IT Security
Department: Information Technology

Job Purpose

The Senior IT Security Specialist will support the design and implementation of a centralized IT security program and compliance framework that ties together the needs of all Bolder Healthcare Solutions (BHS) service lines. Responsible for execution on multifaceted projects and operations related to IT security strategies, risk management, operational security standards, vulnerability management, incident response, and providing IT security and risk focused consultation to the organization as needed. Completes tasks designed to ensure security of the company's systems and information assets.

Education and/or Experience

- Bachelor's degree in Computer Science, Management Information Systems, Information Technology, Business Administration, or other related discipline from a four (4) year college or university
- Certified Information Systems Security Professional (CISSP) certification, or other information security related certification (e.g., CRISC, CISA, GSEC, etc.)
- At least four years of information security experience
- Familiarity with network security, vulnerability scanning, and SIEM technologies
- General understanding of information security management frameworks such as ISO 27001, COBIT, NIST SP 800-53, and ITIL
- Prior experience performing information asset inventory activities and information security risk assessments
- Familiarity with relevant legal and regulatory requirements such as Payment Card Industry / Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX)
- Prior experience performing and/or managing SOC 2 Type 2 and PCI audits
- General understanding of business continuity management and disaster recovery best practices
- Prior experience within the healthcare industry is a plus

Duties and Responsibilities include the following and any other duties as assigned by the Director of IT Security.

1. Supports the evaluation, design, and implementation of the centralized IT security program for all BHS service lines.

2. Researches and provides recommendations to the centralized IT infrastructure team to simplify management of resources and tools used to manage IT security and compliance efforts.

3. Assists with projects and programs needed to address IT security issues. Participates in the governance of those projects and programs, monitors progress and assists with time sensitive issues and decisions.

4. Works closely with BHS IT and application development teams to design secure solutions and applications, facilitating the implementation of protective and mitigating controls.

5. Responsible for managing relationships with external auditing firms for IT security and compliance efforts such as SOC 2 Type II, ISO 27001, and PCI audits. Ensures compliance requirements are met, along with proper artifact and evidence collection and storage to validate adherence.

6. Supports the development and operation of security awareness initiatives, aligned to the BHS strategy necessary for compliance across each of the service lines.

7. Performs quarterly internal vulnerability scanning activities and communicates the critical results to BHS executive management. Advises IT and service line focal points of methods to remediate vulnerabilities, implement compensating controls, and evaluate risk awareness. Develops and tracks metrics and measures to evaluate the implementation of compensating controls and keep management informed of status.

8. Responsible for assisting the Director of IT Security to implement a process for proactively monitoring network endpoints, firewalls, intrusion prevention and detection systems, security logs, and other security alerts. Drives operation of the Security Information and Event Management (SIEM) solution after implementation.

9. Coordinates the annual information asset inventory process. Responsible for working closely with each of the BHS IT and service line focal points to help them perform this process in preparation for completion of annual risk assessment activities.

10. Assists with the implementation of the IT security risk management function, including processes, tools and systems to identify, assess, measure, manage, monitor, and report risks as it relates to information security. This includes supporting the annual HIPAA Risk Assessment and individual service line risk assessments.

11. Responsible for facilitating the information security risk assessment process, including risk remediation, and governance of the risk acceptance process. Manages the risk acceptance process to ensure the implications of risk acceptance are understood, risks are accepted at the right level within the company, and risk acceptances are tracked and reported on throughout their lifecycle.

12. Leads internal audits of the centralized IT security program. Develops audit test plans, performs testing, documents results, communicates results to management, facilitates the creation of remediation plans, works with IT and service line focal points to ensure remediation plans are implemented, and keeps management informed on progress of remediation activities.

13. Responsible for the creation of and delivering metrics for IT security operations and incident response.

14. Manages all information security vendor and supplier relationships and identification of risks related to information security. Performs due diligence to ensure security safeguards are included in the assessment process.

15. Responds to security events by researching the symptoms of the event and working with all parties involved to determine the priority, cause, and resolution. Documents and communicates information security events to peers, management and other IT areas to ensure all parties are aware of risk level and the impact on the overall information security posture of the company.

16. Responsible for documentation lifecycle of the centralized IT security program policies, standards, and procedures. Ensures that these documents are aligned with business, compliance, and risk goals. Creates documentation in the form of policies, procedures, and standards associated with the centralized IT security program.

17. Helps ensure that BHS data, information, and assets are kept secure within an acceptable risk / cost model.

18. Works with project managers to ensure security is included within IT projects.

19. Supports the development of an enterprise-wide business continuity and disaster recovery program, including the maintenance and testing of that program, and the corporate emergency preparedness program.

20. Participates in regular mock-disaster exercises to test the adequacy of existing plans and strategies, updating procedures and plans annually.

21. Participates in investigations and fact finding reviews when breaches occur within the centralized IT security program and recommends corrective action plans to ensure mitigation activities are implemented.

22. Analyzes potential impact to the company for all new security threats and vulnerabilities; communicates risks to all impacted service lines.

This is an exempt position within the Company, requires working overtime as necessary, and may require occasional travel.

Skills

- Detail oriented
- Strong oral and written communication skills with the ability to build and maintain relationships in a cross-functional environment
- Possesses both technical and project management experience including exposure to implementing information security on Windows, Linux, and AS400 platforms
- Ability to work both as an individual and in a team oriented environment
- Demonstrates flexibility to quickly adapt to changing business needs and processes and ability to deal with changing priorities
- Management of multiple tasks / projects and engagements simultaneously
- Ability to maintain a high level of confidentiality
- Strong organizational and planning skills, resourcefulness, and creative problem solving skills
- Self-managed / self-driven individual
- Advanced knowledge of the Microsoft Office suite of products (e.g., Word, Excel, PowerPoint, Visio, etc.)

To apply online, visit http://bolderhealthcare.com/who-we-are/careers