IT Security Services

What is Your Battle Plan to Fight Cybercrime?

Cybercrime, while impacting other industries over the past 20 years, has now attacked healthcare in a big way. Daily, we read about security breaches in small, medium, and large healthcare organizations that often affect hundreds, thousands, or even millions of people and their private information. These violations occur for many reasons including unidentified holes in a technology infrastructure, lack of knowledge and financial resources to build and maintain a strong IT security program, non-existent policies and procedures governing information security, and uneducated and unprepared users. One thing is for certain: security compromises are a serious threat, and they will continue to occur along with security audits, and six- and seven-figure penalty settlements.

The time has come for executives and boards to step up and work closely with IT leaders to develop a robust battle plan to fight Cybercrime. With more personal, medical, financial, and other critical information now available in electronic form, these leaders must become much more proactive in protecting their organization's data and information assets from known Cybercriminals.

Coker has a team of experienced CIO's, IT, and other technical leaders who understand how to assess, design, build, and maintain robust IT infrastructures geared towards fighting Cybercrime in various healthcare environments.

Security Officer as a Service (SOaaS)

Coker offers a remote SOaaS program to establish and manage an IT security program for clients who lack the required IT security knowledge and have limited budgets. Our program provides an affordable approach based on a 3-, 4- or 5-year subscription program.

Following are the key services included in our SOaaS program:

- Full operational security assessment
- Complete penetration test of all hardware and software
- A report detailing results of the first two activities, a recommended remediation plan addressing high-, medium-, and low-risk issues
- Ongoing monitoring program surveying equipment as frequently and randomly as needed
- 24/7 security officer services
- Annual half-day yearly security assessments

Program Phases:

- Phase 1: Operational Assessment
- Phase 2: Information Technology Assessment (Penetration Test)
- Phase 3: Remediation Report and Action Plan
- Phase 4: Action Plan Implementation (optional, additional expense)
- Phase 5: Security Support and Ongoing Monitoring
- Phase 6: Annual IT Security Assessment

Areas of Focus include:

- Assessing existing IT infrastructures including:
  - Hardware
  - Software
  - Databases
  - Wired and wireless networks
  - Internet connections and data uploads and downloads
  - Desktop devices
  - Mobile devices
- Categorizing current IT security risks and recommending prioritized actions
- Remediating security risks
- Providing data and information security education programs to build staff knowledge and awareness

For further information about Coker Group and how we can help with your IT Security, visit our webiste at www.cokergroup.com, or call 800-345-5829 x2021 to speak with Jeffery Daigrepont, Senior Vice President.

Coker
GROUP
Business Advisors for the Healthcare Industry