Information Security Assessment Services

Overview

The value of information security is often only recognized after a breach or incident has impacted a business and its bottom line. Without specific regulatory guidance, businesses are often unsure of the risk mitigation measures that are appropriate for their industry and threat environment. BPM understands how to balance information security and business needs. Our Comprehensive Penetration Testing service will identify vulnerabilities in your IT infrastructure, allowing you to make well-educated decisions on where to best allocate your resources.

- Comprehensive Penetration Test
  - Red Team/Capture the Flag
  - Application Penetration Test: Web/Mobile/Client-Server
  - Device Penetration Test
  - Password Audit
  - Firewall Ruleset Review
  - Infosec Configuration Review
  - Wireless Penetration Test
  - Social Engineering Penetration Test
  - Physical Security Penetration Test
  - Vulnerability Assessment
- Infosec Program Review/Audit
  - Cybersecurity Culture Audit
- Infosec Risk Assessment
- Infosec Training
  - Social Engineering Awareness
  - Leadership/Governance

Just as we advise our clients, we manage our risks with rigorous processes suited to the sensitivity of the information we handle. As a result of these processes and the dedication of our personnel, we have become one of the most sought after security assessment firms in the business.

Industry expertise includes, but is not limited to:

- Credit Unions: Our services comply with all FFIEC and NCUA guidance and include both comprehensive and targeted controls testing, as well as risk assessment implementation and reviews of documented information security policies and procedures to guide information security program development.
- Healthcare: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, form the basis of federal healthcare information privacy and security rules. In order to fulfill our requirement as a HIPAA business associate we follow the International Organization of Standards (ISO) codes of practice for handling sensitive information, and utilizes best standards and testing processes based on the National Institute of Standards and Technology (NIST). As an assessment-only service provider, we provide health care institutions with the confidence of a truly objective assessment of their regulatory compliance and information security controls. Our services include both comprehensive and targeted controls testing, as well as risk assessment implementation and reviews of documented information security policies and procedures to guide information security program development.
- Banks: We assist banks in ensuring they have the appropriate administrative, technical and physical safeguards in place to protect the security and confidentiality of customer information and comply with applicable regulations. With a record of

service dating from before the Gramm-Leach-Bliley Act (GLBA) was enacted, we continue to assists our many bank clients to effectively balance information security with their business needs.

- Government: To fulfill their missions, federal, state and local government must strike a difficult balance between responding to constituents' needs and maintaining effective information security. Records retention requirements, and the legal information requests that constitute open governance, pose unique information security problems for governmental entities. Our services help government agencies strike the appropriate balance between operational needs and information security requirements. Utilizing guidance from the National Institute of Standards and Technology (NIST) that is applied to all Federal Government Agencies, our extensive assessment and risk management experience help organizations understand applicable regulation and their threat environment in order appropriately manage risks and serve their constituents' needs.
- Utilities: As a critical element in the nation's infrastructure, effective information security for utilities is vital to each organization and the nation as a whole. Since The Energy Policy Act of 2005 and the North American Electric Reliability Corporation's (NERC) subsequent development of the Critical Infrastructure Protection Reliability Standards (CIPS), utilities have worked to define standards to secure their industry and the nation's electric grid. We assist public utilities in adhering to industry standards and managing risks to information systems. Our services thoroughly identify information security risks and assist the development of effective policies and procedures, so that the utility can be confident that it is managing current risks and has the processes in place to meet new threats or guidance.

Would a breach have a negative impact on your business's finances or reputation? Call on us to help provide peace of mind and an understanding of the risks you face.

Contact

David Trepp, M.S.
Partner, IT Assurance
541-687-5222
DTrepp@bpmcpa.com