

Security Assessments

Identifying Risks and Vulnerability

Every business, agency, or organization, uses information technology (IT) to meet and exceed goals and objectives. Today's IT world is filled with threats from hackers, cyber criminals, and even nation states. **Do you know your IT weaknesses and vulnerabilities? Do you know the threat posed to your critical data, brand, operations, and financial viability?**

Ensuring the security of your network and protecting critical data is a challenging process. Conducting continuous penetration testing and vulnerability assessments allows you to know your IT network vulnerabilities and take action to stay ahead of the evolving cyber threat you face.

Healthcare providers handling data governed by Federal Laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) must be especially security aware to protect patient information; communications between doctors, pharmacies, patients, and other healthcare service providers; financial data; and other Intellectual Property (IP). According to the Ponemon Institute's 2014 report sponsored by IBM, the average cost per data record compromised exceeded \$201.00 in the private sector and over \$359.00 for healthcare providers, the highest cost for any industry.

Complying with HIPAA Privacy and Security Rules is challenging for healthcare providers of all sizes and the unplanned expenses of a security breach and breach reporting under HIPAA can be catastrophic to your business.

Trusted Solution Provider

Protecting Critical Information

We understand your needs. Our Cyber Security Analysts have extensive experience identifying IT network risks to critical and sensitive data and have broad knowledge of current and emerging threats.

We have performed hundreds of assessments across the public and commercial sectors over the last sixteen years, and pride ourselves in our ability to make real world improvements to your IT security posture.

Our vulnerability assessments allow you to address HIPAA compliance standards and identifying the cause of current and/or possible security breaches. These assessments also help you to better focus your IT security spending and planning.

Our Cyber Security Analysts utilize industry leading assessment tools combined with proven procedures to gather an accurate picture of your security risks. Our techniques combine vulnerability scanning, penetration testing, manual service interrogation, network traffic examination, and threat analysis to give you knowledge—and knowledge is power in the cyber threat filled world.

Your data is important to us. During the assessment, and while our testing equipment is in transit, CyberDx utilizes encrypted storage devices complying with stringent government standards. This level of security ensures your data is safe and secure at all times.

Security Products and Services

At the conclusion of each assessment, our Cyber Security Analysts will discuss the results and provide the following products:



Comprehensive risk-based vulnerability report detailing all findings.



Identification of any findings violating HIPAA Security and Privacy Rules safeguards.



Specific remediation recommendations to include an estimate on the effort required for implementation.



All the data generated during the security assessment to allow trending and retrospective analysis by your IT staff.

CyberDx can also conduct a variety of social engineering "attacks" to simulate real world intrusion methods and help train employees to reduce network risk. Social Engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Often this is the initial entry method due to the high level of success. CyberDx developed the Army's Phishing platform and improved the capabilities to keep pace with the threat environment. Since 2010, **CyberDx has conducted over 30 Phishing attacks, targeting in excess of 50,000 users**, while supporting the U.S. Army.

About CyberDx

Quantum Research International, Inc. (Quantum) and our CyberDx division, for almost two decades has provided cyber security services for some of the largest and most sensitive networks in the world. Our team of highly qualified professionals build lasting relationships with our customers to help them deal with growing cyber threats to their networks and operations. Our greatest strength is our people – a world class team of cyber defenders and information security experts. This talented team works with one purpose in mind – to help our customers maintain effective IT operations at a time of increasing disruption from hackers and cyber criminals.

Founded in 1987 in Huntsville, AL, Quantum is a private business providing multi-disciplined technical support in a wide range of cyber operations including IT security concept development and planning; cyber threat research and analysis; full-service network security engineering; cyber defense training for users, system administrators, chief information officers (CIOs)/chief information security officers (CISOs) and their staffs, and corporate leaders; and professional Penetration Testing (PENTEST) and Vulnerability Assessment services.

CyberDx is committed to establishing and sustaining operational excellence and striving for continuous improvement in all that we do. We excel at meeting challenging commitments to achieve total customer satisfaction.