6 Reasons You Should Conduct Regular Security Assessments

The digitization of information in today's healthcare industry has improved services and patient care delivery but unfortunately it has also spawned some serious side effects: cybersecurity attacks and breaches.

Today's IT departments must be vigilant in identifying network vulnerabilities before they are targeted by cyber attackers. Running regular security audits for your organization is a must – here's why.

Identify Critical Weaknesses in Your Cyber Security Protections

The first step in any strategic security plan is to know your risks. Security assessments use a variety of techniques and tests to conduct an in-depth audit of your organization's defense measures against various attack methods used by intruders – internal or external. This could be an attacker targeting your network from the outside, a disgruntled employee seeking revenge, or malware. For example, WannaCry proliferated as a result of unpatched software common in many businesses. An assessment identifies those unpatched systems, enabling your team to update software and reduce risk.

An assessment's goal is to identify hidden vulnerabilities, loopholes, and potential gaps in your security architecture. Results will detail everything from shared and accessible access credentials and software version updates needed, to a detailed review of how sensitive information was accessed by analysts – and a presentation of the specific data found. Identification is only step one, though. Security assessments also provide healthcare organizations with a rating of risk severity for each vulnerability, guidance for remediating each identified vulnerability, and the opportunity to retest to assess your remediation efforts.

Ensure Sensitive Data is Secured in Your Local Environment

All protected health information (PHI) and electronic PHI (e-PHI) that a healthcare organization creates, receives, maintains, or transmits must be secured and protected. Additionally, all methods of storing and transferring PHI, including databases, servers, connected medical equipment, mobile devices, and cloud storage, need to be regularly evaluated.

Security assessments can routinely test if implemented security measures are properly protecting sensitive and confidential information from all potential points of attack. A range of service options are available, including internal and external penetration testing, database security assessments, and web application testing.

Meet Compliance Requirements and Be Prepared for Audits

The HIPAA Security Rule requires all covered healthcare organizations to demonstrate and document a regular vulnerability scan to assess healthcare devices, applications, and networks for vulnerabilities, exploits, and security weaknesses. HIPAA further requires covered entities to evaluate the likelihood and impact of potential risks to e-PHI and implement and document appropriate security measures to address those risk areas. Overall, Health and Human Services requires that protected PHI is secured against "reasonably anticipated threats to security or integrity of the information" and that you maintain "continuous, reasonable, and appropriate security protections."

Security assessments vary in complexity and methodology. Your organization can choose from a range of services suited to your needs, including vulnerability scanning, penetration testing, social engineering, database assessments, wireless testing, web application testing, and more. Documenting all security and privacy policies during an assessment will serve as an essential reference for procedural audits, and an excellent training foundation for employees. However, with today's advanced hacking and cyberattack methods, compliance does not guarantee security. Regular (at least annual) assessments ensure your organization stays in front of HIPAA requirements and will identify areas beyond compliance that need to be addressed to meet industry cybersecurity best practices and standards.

Identify Budget and/or Training Needs

Security assessments enable your IT team to identify areas of weakness and opportunities for growth in security protection. Understanding where current vulnerabilities exist, and which are priority, allows your IT team to make better informed decisions about future security expenses. Assessments provide the documentation needed to justify or guide your IT department's security budget and validate that budget for the rest of the organization.

Assessments also allow healthcare organizations to foster a healthy internal dialogue and encourage diligence throughout the company. Your employees play the single most important part in network security. Social engineering and other assessments can provide an avenue to identify additional training or resources needed for employee education and compliance.

Develop Contingency Plans

Another advantage of conducting regular risk assessments is the opportunity to develop contingency plans for when disaster strikes. Whether your data is stored on-premise, in the cloud, or both, developing a strategic back-up plan is an essential part of your disaster recovery and overall security plan.

During a policy review, identify what information is or needs to be backed up and how, develop procedures to restore backups following a breach, and standard processes for regular testing of those restore procedures.

Update and Strengthen Cybersecurity Policies and Procedures

A strong security posture includes, but is not limited to, the technical tests we've discussed so far. Your organization also needs good policies and procedures in place across the entire company. You can't afford a piecemeal approach to protecting PHI and administrative data. The costs of data breaches and their consequences including reputation loss, fines, and lawsuits, can cripple a healthcare organization of any size.

With a strategic security assessment, your organization can engage industry experts to review, update, and enhance your organization's cybersecurity policies and procedures including:

- Access control and user account management
- Information security governance and risk management
- Improved workstation and device security
- Business continuity and disaster recovery planning
- Cryptography
- Physical (environmental) security
- Network and operations security
- Security architecture and design

After this comprehensive review, your organization will be equipped with the steps needed to strengthen your overall security posture and can gain peace of mind knowing you've taken advanced steps to minimize your risks against threats.

Ready to schedule an assessment? To learn more about how ENA's security assessment services can help protect your data, visit www.ena.com/security/security-assessment-services.

About ENA by Zayo

ENA delivers transformative connectivity, communication, cloud, cybersecurity, and technology services. Our 99% customer satisfaction rating and world-class net promoter score (NPS) demonstrate our commitment to delivering exceptional customer care. For more information, please visit **www.ena.com**, call **866-615-1101**, or email **info@ena.com**.

ena® by zayo