PROTECT YOUR BUSINESS & PHI

THE BOTTOM LINE

PROTECT YOUR PATIENTS' MOST SENSITIVE DATA

KEEP PACE WITH CHANGING REGULATORY REQUIREMENTS

ACHIEVE COST SAVINGS THROUGH TOOLS RATIONALIZATION

ESTABLISH A SECURITY-DRIVEN ORGANIZATIONAL CULTURE

Attackers want PHI. Make sure your security posture not only meets regulatory compliance requirements but is able to adapt and scale with an ever-evolving threat landscape.

SECURITY STRATEGY EVOLVED

Know your threats. Secure your systems and data, while improving efficiency in your organization.

Are you keeping pace with change?

Healthcare organizations represent an extremely attractive target for cyber criminals due to the wealth of personally identifiable information they maintain. Unfortunately, many in the healthcare industry lack the necessary understanding of data privacy and security risks, or knowledge on how to improve their enterprise security posture. An inability to keep both protected health information (PHI) and organizational data secure can lead to serious financial, operational, and reputational consequences for the organization.

It is only with thoughtful investment in information security that healthcare payers and providers will be able to prepare for new risks and responsibilities, while maintaining patient confidence and profitability. Consider:

- How well do you understand the threat landscape and your areas of vulnerability?
- Do you have adequate security tools and processes in place?
- How are you measuring the effectiveness of your defenses?
- Do you have a roadmap to mitigate your risks and continuously improve your security program as threats evolve?
- Does the board understand the importance of security in today's market?
- Is security aligned with your business strategy?

A strategy that works

Many healthcare organizations view security as a cost center intended to satisfy HIPAA compliance; however, the threat landscape evolves much faster than government regulations and being HIPAA compliant is no longer enough to protect your data and your reputation. In addition, these organizations may be overlooking the additional value an effective security program can bring.

Others realize the important role security plays but their efforts are misguided, with an expectation that more security tools will protect them. The truth is traditional security tools are not enough to stop today's advanced attack methods. It is no longer a matter of if, but rather when, your data will be targeted. A new approach is needed.

Our Security & Infrastructure experts take a risk-based approach to protecting your organization and provide solutions that address the specific threats the healthcare

WE DON'T JUST POINT OUT YOUR VULNERABILITIES. WE IDENTIFY YOUR ACTUAL THREATS AND SET YOU ON A PATH TO ONGOING SUCCESSFUL RISK MANAGEMENT.

industry is facing as the new target of sophisticated attackers. Where other security firms approach security with a one-size-fits-all model, we recognize that each of our clients have different business objectives and risk tolerances to consider. Our uncommon blend of industry and security experts helps you find the right balance to mitigate your risks effectively.

World-class security offerings

West Monroe Partners helps healthcare organizations improve their security posture and reduce the likelihood and impact of potential security threats. With a deep understanding of the healthcare industry and the threats organizations face, we recognize that security is not solely an IT problem and provide solutions covering people, process and technology across the enterprise. Our security offerings are designed to improve our clients' ability to identify, detect, protect, respond to and recover from potential security incidents.

In addition to helping protect valuable PHI data, and ultimately your reputation, our approach improves collaboration between the business, IT, security and compliance teams and helps non-technologists in your organization understand and participate in cybersecurity conversations. Security is then aligned with your business objectives when making strategic decisions.

Initiatives to improve security can be beneficial to the business:

- Consolidation of data sources may drive an established 'source of truth'
- Upgrading technologies to be compliant with security may result in realization of new features and capabilities
- Cost savings via application and/or tool rationalization
- Foster collaboration between business, IT, and compliance

Security Strategy & Roadmap

Our security experts identify your current security posture and then align security with your business objectives in order to determine the appropriate desired state.

We then provide a strategic roadmap to guide you towards your desired state with prioritized initiatives designed to mature controls and reduce the likelihood and impact of potential security incidents.

Our solutions cover people, process and technology to set you on a path to continually improve your security posture. We emphasize security as a component of a healthcare organization's risk management approach and focus on strategic solutions, helping you operationalize your security investments

Cybersecurity Tools & Threat Analysis

We help healthcare organizations optimize their cybersecurity tools and supporting processes to improve their ability to identify, detect, protect, respond to and recover from potential security incidents. With a deep understanding of the healthcare industry and the value of PHI data, we review each tool and provide a detailed report of coverage, configuration and process that highlights whether:

- The tools are the appropriate for the function they perform
- The tools have been deployed and configured appropriately
- Policies and procedures are in place for maintaining the tools over time

In addition to improving the security strategy of the organization, our clients also benefit from understanding when to upgrade to technologies that offer new features and capabilities.

A customized security and tools strategy, based on your business and industry needs, ultimately helps you create an entire organizational culture focused on security. That's business in the right direction.