CASE STUDY

RiverSpring Health™
Live Forward

Contributor:

David Finkelstein
Chief Information Officer

LeadingAge™ CAST
center for aging services technologies

The LeadingAge Center for Aging Services Technologies (CAST) is focused on accelerating the development, evaluation and adoption of emerging technologies that will transform the aging experience. As an international coalition of more than 400 technology companies, aging-services organizations, businesses, research universities and government representatives, CAST works under the auspices of LeadingAge, an association of 6,000 not-for-profit organizations dedicated to expanding the world of possibilities for aging.

For more information contact:

Zohra Sirat, Project Manager, CAST
zsirat@LeadingAge.org
(202) 508-9438
LeadingAge.org/CAST

BLUE ORANGE® COMPLIANCE

Ongoing Penetration Testing is Key to Comprehensive Security and Privacy Compliance

Categories

1. Enhanced System Security and Information Privacy
2. Staff Education about Data Security and Privacy, and their practices
3. Improved Compliance
4. Avoiding data breaches and consequent penalties

Organization Name

RiverSpring Health

Organization Types

Skilled nursing care, post-acute short term rehabilitation care, managed long-term care, assisted living programs, senior housing, and specialized services such as elder abuse prevention and memory care.

Other Partners

BlueOrange Compliance: BlueOrange Compliance has been providing privacy and security assessments since the inception of HITECH, and has over 50 years of experience in technology security, compliance and healthcare. Our national client base consists of hospitals, physician provider practices, LTC Pharmacies, SNFs, LPCs, homecare and hospice and business associates. If you want to learn how BlueOrange Compliance can help you turn HIPAA complexity into HIPAA compliance, call today and speak with one of our security navigation experts.

Organization Description

RiverSpring Health is an internationally recognized non-profit geriatric care organization offering a full continuum of senior care ranging from modern apartments for independent seniors to the most intense level of nursing care, serving more than 10,000 older adults in greater New York.

Since its founding in 1917, RiverSpring Health has grown to include a long-term residential elder care facility located on 32-acres along the Hudson River, a senior housing community with both luxury independent living apartments and assisted living, and a community services division offing a full spectrum of in-home geriatric care, supportive services, and managed care plans for people living at home.

The Challenge

In today's world of cyberwar, many healthcare organizations are implementing penetration testing as a way to evaluate the true effectiveness of their technical controls. Penetration testing can help identify vulnerabilities in an effort to determine the likelihood of real-world threats against an organization's IT assets and physical security, and pinpoint remediation strategies.

The Healthcare security landscape is facing a rising threat of malicious attacks that target protected health care information and/or personally identifiable information. The number of incidents that evade traditional security defenses are increasing at an alarming rate, and with the growing prevalence of EHRs and other online information systems, the playing field has become more enticing to hackers. According to a May 2015 Ponemon Institute study, criminal attacks on healthcare data are up 125% compared to five years ago, and the average cost of a data breach for healthcare organizations is estimated to be more than $2.1 million.

Protecting patient information is a core measure of HIPAA compliance, and proper protection of that information includes Network and Security Systems testing and remediation. However, it can be very difficult for many Healthcare organizations to test and analyze network vulnerabilities. Most Healthcare IT Departments simply do not have resources or expertise that need to be dedicated to the design and implementation of testing methodologies that actively analyze their systems for technical vulnerabilities. In response, many Healthcare providers have partnered with outside expertise to help pinpoint real risks to their networks, assess the performance of their overall security controls, and provide remediation support and guidance. RiverSpring Health has partnered with CAST Supporter BlueOrange Compliance on this project.

Project Description

The IT professionals at RiverSpring Health recognized the potential threat and partnered with BlueOrange Compliance for the solution. For nearly 100 years, RiverSpring Health has been one of the nation's leading Senior Care organizations, and has continually renewed and expanded its commitment to provide the best possible care and the highest quality of life for older adults. Located on 32 acres along the Hudson River in Riverdale, New York, RiverSpring Health provides a full range of care solutions including skilled nursing care, post-acute short-term rehabilitation care, managed long-term care, assisted living programs, senior housing, and specialized services such as elder abuse prevention and memory care.

In the role of Chief Information Officer for RiverSpring Health, David Finkelstein considers maintaining HIPAA compliance a leading challenge. David determined that hiring a compliance partner to perform penetration testing was a "practical approach" to a security challenge, and a "quick and easy way to validate compliance." David goes on to say that he selected BlueOrange because of their "ability to quickly execute the process and use a consultative approach in performing the testing and assisting in remediation." Blue Orange's approach to penetration testing involves a comprehensive and low-touch method: Gather the maximum amount of information in the shortest possible time, work on remediation, and follow-up with increasingly deeper testing.

Implementation Approach

BlueOrange began the penetration testing process by gathering information about the environment, identifying IP ranges, determining the best social penetration testing model and identifying a finite set of email addresses for a phishing campaign. BlueOrange performed an external vulnerability scan remotely, and then came on-site to perform an internal vulnerability scan. Armed with the latest penetration testing tools and techniques, BlueOrange initiated a phishing expedition to attempt to solicit information, and also probed various devices for vulnerabilities and exploitation potential. During the penetration tests, also known as "ethical hacking", BlueOrange simulated the practices and methods of external or internal agents attempting unauthorized data access. Finally, BlueOrange gathered the results and provided RiverSpring Health with a prioritized, detailed and actionable remediation plan.

Advantages to the Approach

Advantages to this approach are:

- This approach is proactive and preventative in nature, rather than retrospective investigation triggered by a cyberattack or data breach.
- Ongoing, as opposed to one time audit/test, which provides opportunities to continue to identify potential vulnerabilities, modifying relevant policies, providing training, monitoring staff compliance, and ensuring security.

Outcomes

Imagine the impact to a Healthcare provider if an attacker were to successfully gain infrastructure access. Security vulnerabilities may be present in operating systems, applications, configurations, or risky end-user practices. That's why penetration testing as part of a comprehensive security and privacy compliance system is so critical to identifying vulnerabilities and ensuring a Healthcare organization is protected.

David Finkelstein concurs, "IT security is not easy, and you need a partner to ensure success." David reported complete satisfaction with the process, depth and level of detail provided by the BlueOrange penetration test. Moreover, he appreciated that BlueOrange "ensured our business was not interrupted by the penetration testing". Finkelstein added that "the BlueOrange penetration testing validated and provided additional insight into potential security risks I had already suspected, and included remediation support and recommendations." Perhaps the most valuable outcome of the testing was the identification of a risk not previously suspected. David Finkelstein reveals that "the spearfishing campaign was eye opening and it identified a vulnerability that required the immediate training and education of all staff across the organization to recognize and report phishing attempts."

Challenges and Pitfalls to Avoid

Staff compliance with new more stringent policies takes time. Make sure to provide staff with education, and engage them in the development of internal policies, testing, refinement, and ongoing training to garner their buy-in. This requires understanding and support from the top level executives as well.

Lessons Learned

Communication and staff engagement in the overall testing, vulnerability identification, and remediation, especially the development of internal policies, is key to getting the buy-in and eases compliance of staff. Ongoing monitoring helps reinforce the initial buy-in.

Advice to Share with Others

Healthcare providers are legally and ethically obligated to ensure patient privacy. HIPAA law mandates documentation, processes, and security controls that must be implemented to protect privacy and security of health information. Complex, ever-changing regulations, increased vulnerabilities and cyber warfare make it difficult to stay in front of emerging threats. Penetration testing provides a realistic view of the actual security state of an environment, insight that is critical to organizations that want to protect and secure their business. In fact, so vital that Finkelstein insists that "Penetration testing should be executed on a routine basis, rather than once every few years". When asked what insights he would share with other Healthcare providers, Finkelstein concludes, "Don't underestimate the complexity of IT security and the necessity of 3rd party validation that you are compliant and secure.".