Considerations for Contracting with Cybersecurity Firms

By Barbara A. Glondys, MHA, RHIA, CHPS

On March 28, 2016, the information systems at 10 MedStar Health hospital locations were attacked by a virus that prevented certain users from logging in to the organization's information systems. The organization immediately moved to back-up systems using paper transactions. All facilities remained open and no protected health information (PHI) was compromised. The attack was widely covered in the press.[1]

At the time of the attack, MedStar Health posted the following statement on Facebook:

> MedStar acted quickly with a decision to take down all system interfaces to prevent the virus from spreading throughout the organization. We are working with our IT and cybersecurity partners to fully assess and address the situation.[2]

In an April 6 post on its website, MedStar Health further credited its partnership with a cybersecurity company for its rapid response and recovery to the malware attack on its information systems. The company wrote that its partner, "… a global leader in cybersecurity, has been on the ground from the start of the situation and has been conducting a thorough forensic analysis, as they have done for many other leading companies around the world."[3]

This successful response emphasizes the benefits of a strong partnership with a cybersecurity firm to ensure both the highest level of security possible, immediate response to compromised systems and untoward events, and thorough mitigation activities.

Authors of a recent *Journal of AHIMA* article also suggest considering an outside firm as part of a cybersecurity plan in the article "Understanding Cybersecurity: A Primer for HIM Professionals." The authors recommend hiring an outside firm to conduct technical and non-technical evaluations, which can include:

- Conducting a vulnerability scan of external-facing systems
- Running a penetration test of key applications and systems
- Evaluating policies, procedures, and organizational practices pertaining to the IT environment[4]

Healthcare organizations face threats from cyberattacks that are increasing in number, frequency, and sophistication. At the same time, demands to better protect health information and meet privacy legislation are growing. Yet providers are being incentivized to provide easy access to health information directly to patients through patient access portals. These conflicting pressures require well-informed and vigilant attention to all aspects of electronic patient information management.

As the authors of an *Information Age* article on outsourcing security services from April 2015 state:

> When it comes to IT security, very few organizations have the luxury of being able to have it all. The reality for most is careful prioritization of security needs, coupled with strategic technology investments to deliver the highest levels of security for the budget available. With the modern threat environment growing all the time and resources at a stretch, Chief Information Security Officers (CISOs) are naturally exploring all options that would allow them to achieve their security goals within the budget available.[5]

The Ponemon Institute's "State of Cybersecurity in Healthcare Organizations in 2016" survey of IT and IT security practitioners in a variety of healthcare organizations looks at barriers to cybersecurity. Respondents said the following factors kept their organizations from having a fully effective cybersecurity posture:

- Insufficient staffing (73 percent)
- Insufficient budget (65 percent)

- Lack of in-house expertise (47 percent)
- No understanding of how to protect against cyber attacks (39 percent)[6]

These deficiencies, if applicable to an organization, further point to a potential need for partnership with a cybersecurity firm. Another *Information Age* article from March 2016 notes that "One increasingly viable option is to outsource security either in part, or in its entirety. By deploying security software as a managed service, organizations can benefit from specialist security knowledge, while handing off all issues associated with the deployment, management, and monitoring applications to a trusted third party."[7]

The increasing number and complexity of cyberattacks has made many organizations realize the advantages of outsourcing their IT security to expert partners.

The IT department, along with HIM, corporate compliance, risk management, privacy and security officers, and human resources, should carefully consider outsourcing certain security services and partnering with cybersecurity firms that best meet the needs of the organization. Numerous companies provide comprehensive security technology and support services.

Cybersecurity firms can provide services such as:

- Security, network, and application performance monitoring
- Detection of internal and external threats
- Network traffic surveillance
- Auditing of actions made with electronic PHI from across the organization's network
- Sending alerts based on unexpected network usage patterns and security policy violations
- Discovery and profiling of new and unauthorized network devices
- Identity management and authentication
- Encryption application to data at rest and data in motion
- Intrusion detection and prevention systems
- Anti-virus and anti-malware programs
- Virtual private networks
- Web application firewalls
- Penetration testing
- Endpoint security solutions
- Anti-DDoS solutions
- Data loss prevention

Support services provided by cybersecurity firms include:

- Security risk assessments
- Policies and procedures
- Workforce education
- Security information and event management

Choosing the Right Partner

In addition to careful selection of the technology and services that best meet the needs and budget of the organization, other considerations include customer service reputation, past performance (references), flexibility in delivery, and purpose-built solutions that have been developed by the company.

Results of a recent security risk assessment may be a good starting point for determining the need for working with an external company and the areas that could be improved through this type of partnership. A security firm can assist with providing an objective security risk assessment to reveal threats and vulnerabilities that need intervention—before it's too late.

Notes

[1] Butler, Mary. “Concerns About Ransomware Rise as Attack Rates Climb.” *Journal of AHIMA*. April 27, 2016. http://journal.ahima.org/2016/04/27/concerns-about-ransomware-rise-as-attack-rates-climb/.

[2] MedStar Health. “Early this morning, MedStar Health’s IT system was affected by a virus…” Facebook. March 28, 2016 [Accessed May 19, 2016]. www.facebook.com/MedStarHealth/posts/10153623370699397.

[3] MedStar Health. “MedStar Response to Incorrect Media Reports.” Press Release. April 6, 2016. www.medstarhealth.org/mhs/2016/04/06/medstar-response-incorrect-media-reports/#q={}.

[4] Dill, Mark W. et al. “Understanding Cybersecurity: A Primer for HIM Professionals.” *Journal of AHIMA* 87, no. 4 (April 2016): 46-51.

[5] Green, Chloe. “To outsource or not to Outsource – How to know if you need Managed Security Services.” *Information Age*. April 9, 2015. www.information-age.com/it-management/outsourcing-and-supplier-management/123459294/outsource-or-not-outsource-how-know-if-you-need-managed-security-services.

[6] Ponemon Institute. “The State of Cybersecurity in Healthcare Organizations in 2016.” February 2016. http://cdn5.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf?elq_mid=1633.

[7] Green, Chloe. “6 things you should consider before selecting a security partner.” *Information Age*. March 15, 2016. www.information-age.com/technology/security/123461105/6-things-you-should-consider-selecting-security-partner.

Barbara A. Glondys (barb.glondys@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Glondys, Barbara. "Considerations for Contracting with Cybersecurity Firms" *Journal of AHIMA* 87, no.7 (July 2016): 40-41.