GRAHAM COMPANY

APRIL 10, 2018

ASK THE EXPERT: CYBER RISKS DURING MERGERS & ACQUISITIONS

Why are cyber risks heightened during mergers & acquisitions (M&A)?

There will always be heightened risk when two organizations' information security programs merge, because the likelihood of a breach increases as the total cyber footprint expands. An August 2017 data breach at a Philadelphia-based health group gave hackers access to the files of 300,000 patients, exposing private data including names, addresses and even social security numbers. The breached health group had recently completed a merger – and while the exact type of system failure that allowed this cyberattack to occur cannot be identified, this incident does shed light on cybersecurity, a potential liability that is often overlooked during M&A.

What are the potential cyber concerns of M&A?

It is important to understand that if the acquired organization has sub-standard safeguards, the acquiring company is at a greater risk of being hacked. During an acquisition, the damages resulting from a breach are inherited by the acquiring organization, which could result in significant expenditures. Organizations must also consider how their cyber risks will evolve. The acquiring company should first assess both the amount and the type of data being acquired. If one hospital network is acquiring another, the acquiring company will need to confirm they are able to properly protect an enlarged amount of sensitive patient information and are compliant with applicable Federal and State regulations. Because regulatory standards are determined by both industry as well as Federal and State protocols, the acquired company could also be held to different standards than the acquiring company.

How can cyber risk be reduced during M&A?

Businesses should first develop and implement a thorough plan to assess the risks associated with the acquisition. Any thorough pre-acquisition due diligence process must include a detailed cybersecurity and IT assessment of the organization being acquired. In addition to performing both vulnerability and penetration testing of the new network, a third-party security firm should be brought on to inspect the network for potential threats and bad actors that may have already breached their systems. Next, all employees should be regularly trained to recognize common threats like social engineering fraud and phishing schemes. Email-born threats against employees are the easiest way for hackers to breach an organization, therefore representing the greatest risk. It is critically important that staff is trained to identify and report suspicious emails. Finally, organization executives should work closely with their insurance broker to ensure all cyber threats are properly analyzed and adequate coverage is in place, should a costly breach occur.

MARC D. LEONE, ESQ.
Producer
MLeone@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5330