Lewis Roca
ROTHGERBER CHRISTIE

root9B

3 CYBERSECURITY CONCERNS IN MERGERS AND ACQUISITIONS

BY: KENNEDY & NELSON

FEATURING: ROOT9B

3 CYBERSECURITY CONCERNS IN MERGERS AND ACQUISITIONS

Law360, New York (November 2, 2016, 11:51 AM EDT)—In a typical M&A transaction, the idea is to combine the strengths of the two entities while minimizing their combined liabilities, thus returning growth and profit to the shareholders. Company combinations can occur either as a purchase of the assets of the target company (asset sale) or through the purchase of a majority or exclusive stake in the equity of the target company (stock sale. In the era of the hostile takeover, one defensive maneuver that was always available to a potential target was to swallow a "poison pill."

BACKGROUND

As the technological, economic and geopolitical sands are shifting in the new century, a more pressing issue in the M&A world is not whether a potential target has intentionally swallowed a poison pill, but rather whether one is dormant in its networks or its people. This particular kind of poison pill is of course a cybersecurity liability, and it is a looming risk for M&A teams on both sides of any potential deal. First and foremost, cybersecurity is not just an IT issue for the kids with the overpriced coffee and ironic t-shirts—it is a growing issue for the entire C-suite, board members, underwriters and legal counsel in each and every deal. According to John Harbaugh, COO of industry-leading cybersecurity firm root9B, "The security risks include absorbing unknown vulnerabilities, introducing an already breached network segment, or allowing an adversary the opportunity to target the seller's network using the acquisition as a trojan horse to compromise the buyer." As such, it is advisable to assess the risk prior to any transaction and make sure it is mitigated as much as possible, insured against, and priced into the final value of the deal.

A very preliminary step in conducting a cybersecurity due diligence review is likely not technical in nature. Cybersecurity itself is not solely an issue of software tools and stronger passwords, rather it is an issue of economics, game theory, politics and human behaviors. As an example, imagine that the proposed target company has intangible assets of significant value, for example trade secrets, engineering designs, customer lists, personal identifying information (PII, confidential bids on government programs, or the like. These are the kinds of assets that the target would likely price very highly, and the acquirer might do the same. Assets of this class tend to hold their value based upon their exclusivity—a trade secret is only valuable if it's actually a secret. Unfortunately, there are innumerable threat actors in the cyber space that would agree, both freelance and state-sponsored, equally motivated by profit to be gained, markets to be manipulated, or mischief to be made. As far as the threat actor is concerned, why

buy the entire company when one can just sneak in and take what you want for free? Another irreplaceable intangible asset is the goodwill that is amassed with one's customer base, again an asset that can be priced at a premium in a customer-based industry. But what is the value of the amassed goodwill if it is vulnerable to extinction with a mere keystroke?

As a preliminary step in any due diligence, one might consider examining the assets themselves—are they valuable enough to tempt a threat actor to intervene? If you are a buyer, make sure these assets are secure. If you are a seller, make sure you haven't already given them away to someone for free. If you are a service provider in the transaction, make sure that your client understands the risks at issue. The risk is not entirely limited to intangible assets either, and not all threat actors are in it for the money. So-called hacktivists are likely to target both intangible and tangible assets for political exploitation just as well, as recently illustrated repeatedly in the 2016 U.S. Presidential election. In addition to considering the economic value of any intangible assets, one would do well to consider the ancillary value that a so-called hacktivist might yield from making a political statement based around your company's information.

RISKS

Three fundamental types of risks that one might consider before, during and after the transaction are: external threat actors, insider threat actors and supply chain threats. The external threat actor is the most recognizable from the headlines and Hollywood storyboards—a rogue individual that hacks into your network to cause harm and/or pilfer the crown jewels. The truth is more complicated than that however, as the threat actor is more than likely entirely invisible to your network and your security team. In fact, by most current estimates, that person has probably been inside your network for anywhere between 100 to 200 days before being detected—if he or she is ever detected at all. Put another way, at the commencement of any deal, one of the first considerations on the cyber front should be to make sure there are no unwanted actors inside the network. If they are there, it is necessary to assess where they have been, for how long, and what assets may have been compromised in the process. In a worst case scenario, the threat actor can be sitting idle on the asset during the course of the entire transaction, from opening offer to closing, without ever being detected—and then walk away at his or her leisure with the crown jewels on the day of closing just for fun. Bear in mind that cyberdefense tools are necessary but not sufficient to protect against external threat actors—they adapt to new technologies as fast as they are deployed, which requires persistent monitoring and evolution to ensure the defenses are appropriate.

A second and more insidious threat to consider is that of an insider, for example an employee or contractor of the target company. The insider is not necessarily a proper villain, and can just as easily be naïve or simply untrained on his or her personal security responsibilities. A disgruntled employee is a caricature of an insider threat, an individual who downloads company trade secrets for personal gain or out of self-righteousness. The casual employee that clicks on every incoming spearfishing attempt because he or she is untrained on network security is another, more prevalent, kind of insider threat. Attentive deal makers will attempt to ascertain the risks of each kind of insider threat, both through software tools that can detect likely insider threats based on network behaviors as well as through a thorough investigation of the policies and procedures in place at the target company. Again, the cyberdefense tool against insider threat will lend some assurance that there are no indicators of intentional bad actors, but if there are no company policies, procedures, or trainings on network security for its employees, then every individual who moves from the target to NewCo is one untrained click away from becoming an unwitting insider threat.

The third and most esoteric risk is to the supply chain of NewCo from inadequate security or improper network architecture resulting from the merger or acquisition. Parties should consider what the technological tools and culture of NewCo will look like well in advance of the closing, lest the combined resources of the two companies will yield more vulnerabilities and risk together than they ever did on their own. Furthermore, companies would do well to ensure that the new entity has a defensible network from a systems and controls perspective, and that latent threats do not lead to impending losses. As an example, threat actors have successfully used unsophisticated social engineering techniques (spearphishing for example) to enter business networks and then bridge the gap into physical plant and industrial control systems. A recent example occurred in Germany, when hackers were successfully able to cause physical damage resulting in the shutdown of a steel mill. See e.g., http://www.bbc.com/news/technology-30575104. It should be standard practice at this point to maintain isolation, both physically and sociologically, between the business end of the network and the production and operations side of the network. A merger or acquisition is a perfect opportunity for both parties to make the required changes, both technologically and behaviorally, that can ensure that NewCo truly ends up being safer and more secure than the sum of its parts.

STRATEGIES

According to Harbaugh, “Simply relying on passive assessments, compliance, regulation and industry best practice to measure the security and safety of the acquired network is not sufficient.

The adversary understands these same requirements and will use them as a playbook to compromise the network, understanding that each business most likely only meets the minimum standards to secure their network. This is why it is critical for cybersecurity risks to be considered, evaluated and addressed at the earliest stages of the process using a model that takes into account business-context driven threats, active adversary pursuit and the vulnerabilities or weaknesses being introduced in the acquisition."

The cyberthreatscape moves at a much faster pace than the American regulatory or court system, which is not surprising to anybody who has ever been involved in a merger or acquisition. For better or for worse, the legal and regulatory framework in the U.S. is likely to be reactive rather than prescriptive, thus there will not likely be any agreed upon best practices or reasonable standards by which a board can protect itself. Rather, a deal gone south for cybersecurity reasons will cause some unlucky parties will establish what is clearly inadequate, negligent, or reckless practice; and the rest of the industry will adopt changes thereafter.

That being said, there are several actions that companies on both sides of the transaction can take to try and minimize the risk of setting the bar for reasonableness. First and foremost, companies should recognize that cybersecurity is a governance and risk issue, not an IT issue, and implement a comprehensive cybersecurity review at the board level prior to engaging in discussions. Secondly, during the due diligence phase of any proposed deal, third party experts should conduct a cyber audit to make sure that the deal is viable and the risk is properly addressed and/or priced. The target's networks and systems should be pentested before and during the negotiations and approvals to make sure that that status quo remains so—remembering that cyber technology can evolve several times during the pendency of a large deal. Additionally, parties might consider purchasing cyberinsurance to hedge against any unforeseen discoveries or events that occur during and/or in the immediate aftermath of the deal.

Finally, and most importantly, both boards should come together to focus on their respective cybersecurity cultures—a more prescient indicator of risk than perhaps any technical undertaking. Do the companies agree on whether cybersecurity is an IT or board issue, a technology tool or a human behavioral issue? If the answer to either of those questions is not a resounding yes, then one of the most fundamental cybersecurity risks facing NewCo is which culture will prevail?

—By Ryan B. Kennedy and William D. Nelson, Lewis Roca Rothgerber Christie LLP

Ryan Kennedy is of counsel in Lewis Roca's intellectual property practice group in Albuquerque, New Mexico. His background includes extensive experience in licensing, patent strategy and portfolio development. He can be contacted at rkennedy@lrrc.com or 505-764-5477.

William Nelson is a partner in the securities litigation practice group in the firm's Colorado Springs, Colorado, office. His background includes securities litigation, securities arbitration and regulatory defense. He can be contacted at wnelson@lrrc.com or 719-386-3057.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Lewis Roca Rothgerber Christie LLP is an Am Law 200 commercial law firm for handling complex matters in litigation, intellectual property, business transactions, gaming, government relations and other practice areas. Offices are located in Albuquerque, Colorado Springs, Denver, Las Vegas, Los Angeles, Irvine, Phoenix, Reno, Silicon Valley and Tucson. Our corporate and securities attorneys provide a wide range of services on behalf of private and public corporations in the U.S. and abroad. We assist with all corporate needs related to structuring and formation, transactions, finance and securities, operational issues, board matters, compliance and tax. Clients range from major international corporations to entrepreneurial start-ups, and we have depth of experience with a broad range of corporate structures, joint ventures, partnerships, franchises and not-for-profit organizations. For more information, visit lrrc.com.

Ranked as the #1 Cybersecurity company for three consecutive quarters by Cybersecurity Ventures (Jan 2016), root9B stands in defiance of the unwanted human presence within our clients' networks by attacking the root of the problem—the adversary's ability to gain entry and remain undetected. root9B's application of advanced technology developed through cutting-edge R&D and engineering and refined through relevant, hands-on training is revolutionary. root9B combines cutting-edge technology, tactics development, specialty tools, and deep mission experience. root9B personnel leverage their extensive backgrounds in the U.S. Intelligence Community to conduct advanced vulnerability analysis, penetration testing, digital forensics, incident response, Industrial Control System (ICS) security, and active adversary pursuit (HUNT) engagements on networks worldwide.
For more information, visit www.root9B.com.