Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

With New Cybersecurity Approach, Can Insurers Meet Demand?

Law360, New York (January 08, 2015, 12:04 PM ET) --

Ben Beeson

In the last 12 months, much has been written about adopting a governance approach to cyber-risks led by the board of directors and executive leadership. Nobody would disagree that a new approach is needed in the face of threats that now have the ability to bring companies to their knees. Many pinpoint seeing a high-profile CEO lose his job following a major data breach as the catalyst for change. However, there is another little discussed reason that is proving to be fundamental in ensuring that companies are better prepared to defend against cyberthreats.

2014 was the year that the mantra "Build Resilience as Prevention is Impossible" came to bear. A major change in cybersecurity thinking is developing but this didn't just happen overnight, it has taken years to come to fruition. It is true that too many in senior management for too long saw cyber-risk as purely a technical problem. This is understandable but many chief information officers and chief information security officers were more than happy to keep it that way, incentivized by budgetary pressures or frankly the fear of job loss. In the face of such a recent onslaught of cyberattacks, many technical leaders now feel emboldened to admit to senior management that they cannot guarantee impregnability.

The importance of this admission cannot be underestimated as, without it, many enterprises would be slower in forcing executive leadership to take responsibility. There is much work to be done, not least in understanding that a "Defense in Depth" strategy is no longer enough. Traditional signature-based defenses such as antivirus software, intrusion detection systems and firewalls that protect the perimeter continue to be important but have proven to be insufficient in keeping attackers at bay. Slow-paced targeted attacks, commonly now known as advanced persistent threats (APTs), more often than not are successfully launched from a social ruse such as spear phishing. A firewall is simply bypassed by such an attack vector. Executives must develop enough technical knowledge to challenge CISOs in developing a threat intelligence and monitoring strategy. Identify the mission critical assets that you wish to protect and seek the capability to understand the adversary who wants these assets. This will then improve your chances of detecting an attack at an earlier stage of the "kill chain" and help minimize the financial loss. Expect the adversary to be already on your network, so harden your defenses and make yourself a more difficult target.

The inability to prevent a sophisticated APT attack is the fundamental reason why insurance increasingly has a role to play as part of a strong risk-management strategy. The federal government recognized this back in the summer of 2013, engaging the industry in the creation of its cybersecurity framework, known commonly as the "NIST Framework." In the absence of legislation from Congress that would impose minimum security standards on industry, how could the government incentivize adoption of a voluntary framework? At that time one such carrot was seen as competitive insurance terms, but this misunderstood the maturity of the cyberinsurance marketplace.

Emerging toward the end of the '90s, a specialist market evolved to address increasing financial risk to industry from handling consumer, patient and employee personal data. Many cite the introduction of California's data breach law, S.B. 1386, in 2003 as the key reason that the market took off. Over the last decade, capacity (insurance available for any single buyer), grew steadily as did total annual premium spend, but it was not explosive growth. Today, it is estimated that there are more than 50 insurers underwriting cyber-risk for U.S. companies, based mainly in the U.S. and London. Total capacity is between $300 million and $400 million. Total annual premium spend is now estimated to be $2 billion. These figures may sound impressive, but relative to other more mature property and casualty classes they are still small.

The primary aim of the NIST Framework is to improve the resilience of the 16 defined critical infrastructure industries against a major cyberattack. In order for insurance to act as an incentive for framework adoption, a commoditized cyberinsurance market had to exist. It is true that with regards to consumer data breach, solutions have become less customized and increasingly look the same. However, and as recently seen with the Sony Pictures attack, sabotage remains a much greater concern to many critical infrastructure industries. Malware can erase corporate data entirely or, much worse, facilitate actual physical damage, as was recently publicized by the German government about a German steel mill. A few specific solutions to address physical damage, business interruption and bodily injury losses from a cyberattack are only now beginning to emerge, but it is early days. The pace of the introduction of these solutions are slowed by those who would prefer to remain silent on traditional property and casualty classes as to whether cyber-risk is covered or not. Certainly regulators are already pressuring insurers to affirmatively cover or exclude, and the picture will become clearer as the losses continue to build. In the interim, as a buyer, ask yourself one question: Has my insurance carrier actually underwritten my cyber-exposure? Particularly relevant to critical infrastructure industries, were any questions asked as to how I seek to secure not just the corporate IT network but also the industrial control systems that we operate?

Clearly the attacks on the retail sector in particular have driven explosive demand for cyberinsurance over the last 12 months. However, ironically, as demand has grown insurers have now started to raise baseline security standards that buyers must meet in order to be considered for coverage. Whereas at the beginning of 2014 it was possible for an organization that accepted payment card data to be PCI DSS-compliant (Payment Card Industry Data Security Standard) to obtain coverage, now insurers want to see enhanced techniques such as tokenization or end-to-end encryption. 2015 will be the first year that we start to see certain buyers declined cyberinsurance and regarded as uninsurable, thereby delivering on the incentive for better security that the government has been seeking. As buyers now increasingly accept the severity of the risk and wish to transfer it, they know that this will only be possible by adopting a strong risk framework such as NIST.

The insurance industry has faced criticism in recent years about its ability to address major emerging risks including environmental, supply chain and reputation. Cybersecurity presents a formidable new

challenge and in the face of increasing buyer demand, the industry must focus on three things. First, it must address, and quickly, the shortage of capacity in the market. For many buyers, $300 million will not be enough, and if anything this is contracting in the retail sector. Congress does not seem willing to provide a backstop to help the market develop so brokers, insurers and reinsurers must work together to quickly achieve $1 billion in availability. Secondly, in the absence of actuarial data to model the risk the industry must continue to innovate and develop solutions. It is good news that in addition to consumer data breach the market is now also starting to address consequential losses from the sabotage threat. However, it cannot be good enough that theft of intellectual property relative to cyber-espionage, and one of the biggest concerns to corporate America, still remains uninsurable today. Finally, there must be much more clarity from both the specialist cyberinsurance market and traditional property and casualty insurers as to what is covered and what is excluded. Silence with no affirmative language can no longer be acceptable, nor can the growing uncertainty about "attribution," and whether insurers might rely on act of war exclusions.

—By Ben Beeson, Lockton Companies

Based in Washington, D.C., Ben Beeson is vice president for cybersecurity and privacy at Lockton Companies. His experience includes working with both the U.S. and U.K. governments to improve industry resilience to cyber-attacks, including assisting the U.S. Department of Homeland Security with rollout of the NIST Cybersecurity Framework.