SANDBERG PHOENIX

PROFESSIONAL LIABILITY BLOG

Corporate Boards Need to Think About Cybersecurity

AUTHOR: SANDBERG PHOENIX

It seems like we can't go a week without hearing about a cybersecurity breach at a major US corporation. Corporate boards need to be aware that improper oversight of cybersecurity issues could lead to a shareholder derivative lawsuit. One such example from within the last couple of years is *Palkon v. Holmes*, 2014 WL 5341880, at *1 (D.N.J. Oct. 20, 2014) (No. 2:14-CV-01234 SRC). *Palkon* involved the global hotel operator Wyndham, which between April 2008 and January 2010 was subject to three cyber-attacks, each resulting in a loss of customer data.

After the third breach, a shareholder filed a derivative lawsuit claiming the board failed to implement adequate data-security mechanisms such as firewalls and elaborate passwords. The plaintiff-shareholder argued this failure allowed hackers to steal customers' data, and that the failure damaged Wyndham's reputation and cost it significant legal fees.

The court rejected the plaintiff-shareholder's claim, noting a variety of ways the board actually had taken steps to defend against cyber-attacks. For example, the board discussed cybersecurity at 14 meetings between October 2008 and August 2012. Additionally, the board's audit committee reviewed the same matters in at least 16 meetings during that period. What's more, Wyndham hired technology firms to investigate each breach and to issue recommendations on enhancing the company's security. After the second and third breaches, Wyndham began to implement those recommendations.

The moral of the story? From what the *Palkon* court found, Wyndham took cybersecurity seriously and avoided liability in the shareholder derivative action. But other boards might not be so fortunate. In this day and age, considering cybersecurity is a critical board function.

By Mohsen Pasha

Mohsen Pasha Image not found or type unknown