Davis Polk

The PetyaWrap Attack, Anthem Data Breach Settlement, and NYDFS Cyber Regulations All Highlight that Companies Should Review Their Access Controls

June 29, 2017 | Client Update | 2-minute read

Three recent cybersecurity events highlight the need for companies to review their access controls to limit who has administrator privileges and how long those elevated privileges last.

First, this week, computer malware that has variously been called PetyaWrap, WannaCry2, GoldenEye and NotPetya began spreading in dozens of countries, encrypting computers and informing users that they could unlock their machines by paying a $300 ransom. Although the malware first appeared to function as ransomware, it now looks to be more akin to a wiping virus. One way that the malware spread across networks is by using a Windows remote execution tool, which depends on infected computers having access to elevated account privileges.

Second, last week, Anthem Insurance reached a record $115 million settlement in a class action lawsuit over Anthem's 2015 data breach. News reports indicate that, like most cyber breaches, the Anthem attack began with a successful phishing attempt. After gaining access to a handful of relatively low-level accounts, the attackers were able to move laterally within Anthem's computer systems and gain access to increased account privileges and vast amounts of confidential data.

Third, the New York Department of Financial Services ("NYDFS") recently implemented new cybersecurity regulations, many of which will become effective on August 28, 2017. Under these new rules, companies that are regulated by the NYDFS must limit user access privileges to their computer systems and must periodically review such access privileges. *See* 23 NYCRR Part 500.07, our recent webinar on the NYDFS cyber regulations, and our blog at www.cyberbreachinfo.com.

Taken together, these three events illustrate the need for companies to consider whether their access controls could be improved. For example, as part of its post-breach remediation efforts, Anthem agreed to:

- Implement two-factor authentication for remote access to its computer systems;
- Limit users' access to the data systems that are necessary for their job functions;
- Require users to obtain management approval for certain administrator privileges or access outside the scope of their normal responsibilities;
- Ensure that elevated privilege access is provided for a defined and limited period of time, with persons having to reapply to extend their privileged access; and
- Automatically terminate user sessions after a limited period of time rather than allowing them to continue indefinitely.

In general, restricting administrative permissions by person, location, and/or time can, in many instances, significantly mitigate the damage associated with a cyber attack by preventing a malicious person or software that has penetrated a company's computer system from moving freely through networks and gaining access to additional credentials and data. For companies that are subject to the NYDFS regulations, the specific access controls that are adopted should be informed by the risk assessment required by 23 NYCRR Part 500.09.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Neil H. MacBride
+1 202 962 7035
neil.macbride@davispolk.com

Antonio J. Perez-Marques
+1 212 450 4559
antonio.perez@davispolk.com

Neal Potischman
+1 650 752 2021
neal.potischman@davispolk.com

Gabriel D. Rosenberg
+1 212 450 4537
gabriel.rosenberg@davispolk.com

Margaret E. Tahyar
+1 212 450 4379
margaret.tahyar@davispolk.com