CLIENT ALERT

Risks Posed by Third Party Vendors Increasingly a Challenge for Businesses

Aug.23.2017

This week it was reported that Indian police arrested four people accused of leaking a pre-release episode of the blockbuster HBO show, "Game of Thrones." The leak is supposedly the result of employees from a Mumbai-based company that stores and processes the series for the Indian streaming website Hotstar.

These arrests—which appear unrelated to the recent and well-publicized corporate hack of HBO—underscore the challenges that businesses operating around the world face in safeguarding their intellectual property in the supply chain. Many corporations rely on third party vendors to deliver their business services and products—in this instance television content—around the world. Yet, the security capabilities of these vendors varies widely, which is why companies can and should take key steps to protect their sensitive information as they share it with these third parties.

The two primary threats that third party vendors pose to companies are: (1) ensuring strong cybersecurity protections to mitigate the chance of a damaging hack; and (2) minimizing the chance of theft of sensitive business information by insiders with access. To address these concerns, companies should consider the following.

Mitigating Third Party Cyber Risks

First, any arrangement with a vendor should make clear in the contract that the vendor requires appropriate information and network security, either a specific standard (*i.e.*, National Institute of Standards and Technology) or standard commercial standards. Depending on the nature of the business information being shared with the third party, the contractual provisions can be more or less prescriptive. Such a provision will ensure that the third party vendor is thinking diligently about security. That, together with a strong indemnity clause and rejection of any limitation of liability provision, also helps protect the company from liability in the event of an incident.

Second, businesses should ensure they have the ability to conduct or request regular (at least annual) audits of a vendor's information systems. Conducting audits of contractors, particularly when sensitive information is involved, is good way to identify a cybersecurity problem before it causes damages.

Third, businesses should require any third party vendor to promptly notify the company of a breach–broadly defined–and also mandate the ability to conduct joint (and privileged) investigations. If a breach is not avoided, then ensuring investigations are done quickly and correctly–without wasting time arguing with the vendor about a company's rights–is an important way to mitigate any damage.

Guarding Against the Insider Threat

Insider threats pose their own unique set of challenges, as the recent theft of the Game of Thrones show demonstrates. From stealing classified government information to ripping off a company's trade secrets, employees with access pose unique

concerns. But these, too, can be mitigated by taking a few key steps, and making sure important third party vendors do the same.

First, limit employee access to sensitive information. Time and again employees have far more access to company data than they need. Limiting both ordinary user access and the much broader "administrator" access is critical.

Second, make it harder for workers to actually steal sensitive information. Limit the ability to download programs on work systems that allow for file sharing, such as Dropbox. Only permit the use of USB drives to remove data when it is mission critical to a certain employee's job. Don't let employees access their personal email accounts at work, which is both a good cybersecurity practice and also one that limits their ability to send files from an unmonitored account.

Third, appropriately monitor the network, particularly when it comes to accessing sensitive information. A company or vendor should know when a huge download of data from the network occurs, or when a user is accessing a sensitive location of the network that they have no reason to access.

There is no sure way to block every cyber-attack or keep every insider from stealing sensitive data. But these are important precautions and companies are wise to consider these steps for themselves and the third party vendors on which they rely.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com