Blogs
December 13, 2021
Public Chatter

# FBI Warns Your Deal Might Be Threatened by Ransomware!

Here is a crazy thing to be aware of. Ransomware actors are targeting companies involved in significant, time-sensitive financial events. Cyber criminals identify non-publicly available information, which they threaten to release in an effort to entice victims to comply with ransom demands. That's right. Your deal - including an IPO - could be used against you. In most cases, the initial intrusion comes through trojan malware. Related to this is this **recent FBI notice** that significant, publicly disclosed financial events are targets for ransomware attacks. So you might consider reviewing your company's information security practices ahead of any deals. Beyond the obvious security protocols a company should have (egs. back-up critical data / ensure your anti-virus software is up-to-date / limit access to sensitive information to those who need to know): Here are a few basic tips that could help in protecting your company from a governance perspective: 1. Implement an information security program appropriate to the company's risk levels, including through ensuring appropriate reports by the chief information security officer to, and oversight by, the board of directors or a specified committee

---

2. Flag information about potential deals as confidential data subject to higher levels of security protocols

---

3. Train (and refresh) employees on best information security practices – like not using public wi-fi networks when accessing sensitive information, spotting malicious emails, etc.

---

4. Confirm your outside legal, financial and other representatives use best practices for securing information

### Explore more in

Corporate Law
Blog series

## Public Chatter

Public Chatter provides practical guidance—and the latest developments—to those grappling with public company securities law and corporate governance issues, through content developed from an in-house perspective.

View the blog