WAS CHRYSLER'S VEHICLE HACKING RISK AN SEC DISCLOSURE REPORTABLE EVENT?

[photo: K2D2vaca via Flickr]

Remember the data breach at JPMorgan Chase, exposing 76 million accounts to "hack-mapping"? Last October, JPMorgan Chase publicly disclosed the intrusion and exposure to investors in an 8-K filing with the Securities and Exchange Commission. The statement complied with the SEC's CF Disclosure Guidance: Topic No. 2 – Cybersecurity.

Other companies whose customers' data have been exposed also disclosed breaches in 8-Ks, including Target, TJX Companies, Heartland Payment, EMC and Google. (Firms NASDAQ, Citigroup and Amazon have not.)

Disclosure of known cybersecurity threats or attacks with potential material risks allows investors to make informed decisions. Stock share pricing will fluctuate and reflect the true market value once risk has been factored by investors – and not remain artificially high.

Fiat Chrysler America (FCA; NYSE:FCAU) has known for nearly a year about the risk that Chrysler vehicles could be hacked remotely, according to Fortune magazine Thursday.

Yet to date no filing with the SEC has been made, disclosing this specific cyber risk to investors, customers, and the public.

The SEC's Disclosure Guidance, though, is just that – guidance. There aren't any firm rules yet in place, and the guidance itself was published in October 2011. A lot has happened and changed about technology and cybersecurity risks since then; the guidance has not reflected the increasing threats and attacks to business' data.

Nor does the SEC's guidance distinguish between cybersecurity threats to service products (like banking services), versus hardlines or manufactured goods (like automobiles which offer software as an additional, non-essential feature). The software industry's chronic security patching confuses any distinction; should software companies likewise include all security patches in their SEC filings, or continue as they have without doing so? It's easy to see how revelations about Adobe Flash after Hacking Team was hacked have materially hurt Adobe and all companies relying on Flash – yet Adobe hasn't released a statement at its website. (Only a statement addressing the 2013 threat to customer accounts is posted.)

Are financial services firms any more obligated than software firms? Are automobile companies, which claim ownership of on-board software, any more obligated than software companies?

It's likely FCA chose not to reveal the vehicle hacking threat until efforts to mitigate potential damage had been completed. The now-released security patch for Chrysler vehicles is an obvious indication of this attempt.

Less visible to the public and to investors is any financial effort to reduce future financial exposures. Has FCA established a protocol for

investigating any suspect vehicle accidents? Were reserves set up for future claims should there be (or have been) an accident caused by hacking of their vehicle software?

Can investors adequately account for their own financial risk if they do not know what actions FCA has taken? At this point, investors only know what Chrysler owners and the public know: FCA issued a recall Friday on 1.4 million vehicles at risk, in order to patch their UConnect systems.

Senators Richard Blumenthal (D-CT) announced Friday that he and Ed Markey (D-MA) are working on new legislation, to ensure the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) establish new safety standards for software features in vehicles, in response to the kind threat revealed this week. This is problematic – members of Congress have proven repeatedly they are not able to grasp technological subtleties and details. We'll have to hope for the best.

But business reporting must likewise keep up with technology; the SEC should revisit cybersecurity disclosure guidance immediately, given the size and scope cybersecurity threats pose to the public. Disclosure to investors and the public should not be a hit-or-miss proposition.