What Does Ransomware Cost Companies?

By Eric Begun
King & Fisher Law Group, PLLC

In its 10-Q filing for the quarter ended September 30, 2017, Merck & Co., Inc. stated the following:

> On June 27, 2017, the Company experienced a network cyber-attack that led to a disruption of its worldwide operations, including manufacturing, research and sales operations. … [T]he Company was unable to fulfill orders for certain other products in certain markets, which had an unfavorable effect on sales for the third quarter and first nine months of 2017 of approximately $135 million. … In addition, the Company recorded manufacturing-related expenses, … as well as expenses related to remediation efforts … , which aggregated $175 million for the third quarter and first nine months of 2017.

Worth noting, this $310 million amount likely does not include all legal fees, forensic costs, and all other costs, expenses, and losses related to the cyber-attack. Nor does it appear to include other costs, expenses, and losses that may be indirectly revealed elsewhere in Merck's business or operations. The attack in question is the NotPetya ransomware attack, which impacted countless companies worldwide on June 27 of this year.

Lost Business Resulting from Ransomware

Merck's announcement is remarkable for several reasons, especially for those who negotiate technology contracts and agreements with data privacy and security implications. First, it's noteworthy in its relatively clear quantification of lost business resulting from the ransomware attack. That is, often

it is difficult to quantify lost business, lost sales, and consequential damages when negotiating liability provisions related to data security and information security in technology agreements and other commercial contracts. This is not to say that Merck's recitation of these amounts is a new rule-of-thumb or benchmark, but it may start a conversation.

Quantifiable Losses

Second, the loss numbers reported by Merck are not small ones. It is common to discount publicly announced forecasts of ransomware impacts that are viewed as extreme – $75 billion per year, according to one recently cited resource. But the concreteness of Merck's number and the specificity of the ransomware attack merits attention.

Ransomware is Fact-Specific

Third, the Merck announcement implicitly underscores the criticality of the precise facts surrounding the NotPetya ransomware attack and the unique business and situation of Merck. Not all ransomware or malware attacks can cause the same sort or amount of losses reported by Merck, nor does the same ransomware or other malware give rise to the same quality or quantity of losses for every corporate victim. When negotiating data privacy and data security provisions in commercial technology contracts and similar agreements, it is important for all sides to consider the specific circumstances and risks related to the transaction and parties in question.

Ransomware Impacts Are Not Necessarily Per-Record

And, fourth, the Merck report sheds light on the financial repercussions of ransomware, as opposed to other malware and hacking activities. That is, there are a number of industry and other reports and surveys that speak to the financial and other impacts of data breaches and security breaches on a per-record basis (for example, cost per record, records per breach, etc.). The 2017 Ponemon Institute Cost of a Data Breach Study, Verizon's 2017 Data Breach Investigations Report, and Gemalto's Breach Level Index Findings for the

First Half of 2017 are just a few. However, in many cases the particular per-record numbers reported do not provide a clear picture of the financial effects of ransomware, which often is not the kind or scope of cyber-attack that can be assessed on a per-record basis.

Merck’s 10-Q for the third quarter of 2017 is definitely not a quick-fix answer to the question of how much a ransomware attack would or could financially impact a company. However, for attorneys, contract professionals, and others who draft and negotiate technology agreements and contracts and, specifically, information and data security and privacy provisions, the Merck quarterly report is potentially meaningful.