CORPORATE COUNSEL
An ALM Website
corpcounsel.com | March 2018

litigation costs

DEALING WITH A BREACH'S LONG-TERM FALLOUT

BY STEVEN SCHWARTZ

YOUR CIO JUST CALLED TO LET YOU KNOW there has been a cyberattack and a possible breach of company information. Now what?

At the first suspicion of a cyberevent, some form of triage must begin. The first step is to confirm what happened and when; second, identify the nature and extent of the breach and its potential impact; and, third, determine the immediate remedial steps to keep the company functioning. These assessments are essential for a business to remain operating, fully functional and ready to begin damage control. After this immediate triage, it might be tempting to think that "things are under control." That would be a mistake. Only after the initial assessments are made do the critical longer-term challenges become clear.

Potential follow-on damages demands come after determining what the company needs to disclose to customers, suppliers, shareholders and all others potentially affected by the breach. The costs of the immediate cleanup from a cyberevent are typically dwarfed by the follow-on litigation filed against the company for some form of economic damages.

FAITHIE/SHUTTERSTOCK.COM

Assessing those follow-on claims is critical.

A company can also consider filing claims under its cyberbreach insurance policies for injuries incurred (e.g., business interruption losses). The claims filed against the company, and by the company for reimbursement for losses, can be complex and require substantiation. If not managed properly, there can be a potential conflict between the position advanced by the victim in connection with *its* insurance claim, if misconstrued or not stated accurately, and the defensive arguments advanced in litigation with customers, suppliers and others allegedly injured by the breach. Even when there is no conflict, consistent analysis and arguments can strengthen both affirmative and defensive positions. Early expert involvement is important.

Experience tells us that a breach will likely spawn allegations of damages from individuals and businesses whose private information was compromised. While it is usually challenging for plaintiffs to show actual damages, a variety of novel damages claims have been advanced that assert injury

from the mere threat that confidential information will be disclosed to the public at large, with the potential of some adverse consequences. This is in contrast to typical damage claims that, at least, allege actual injury. Some courts have allowed such claims to go forward. As a part of a consumer class action, the alleged damages can easily become substantial.

Customers and suppliers may allege damages resulting from the potential theft and misuse of confidential or proprietary information. What complicates these demands is that, as with the consumer class actions discussed above, they typically involve damages associated with the *risk* of misuse and injury and not actual damage. Measuring the likelihood that stolen information will be misused and cause injury to its owner is a challenge for plaintiffs who assert claims and defendants who fight them. That said, defeating class certification is an opportunity to make such claims disappear, at best, or minimize their magnitude, at worst. It is critical to understand the demands made by suppliers and customers, to make initial assessments of the risks those plaintiffs might face from a disclosure of confidential information, and to identify strategies to defeat class certification. Economic and market questions can be complex and early involvement by economists and accountants, as appropriate, yields better answers than without such analysis. Determining the merits of these claims as a part of an early assessment helps the affected company identify its exposure and make informed choices about whether financial reserves are appropriate and, more fundamentally, about litigation strategies, including settlement considerations.

In addition to the claims asserted against it, the company may suffer its own injury, as cyberevents can breed customer/supplier distrust that affects sales and costs in the short- and long-term. In the short-term, firms may decide against doing business—or limit the business they do—with a company that suffered a cyberbreach while determining whether the risk of that business relationship is acceptable. Depending on the steps taken by the breached company, there may be either longer-term business interruption or a return to normal business activity. In the aftermath of a breach, an economic or other financial expert can provide assessments of business trends and identify causal relationships between the breach and sales/profit trends. That analysis is critical to an understanding of the impact of the breach. Economic analysis can help determine whether business fluctuations are the result of normal cyclical activity in a market or are exacerbated by a breach. Since those effects can form the basis for business interruption claims, having a rigorous basis for determining what that injury might be improves the economic argument for coverage and support of a claim.

PLAYING OFFENSE AND DEFENSE

A simultaneous offensive and defensive posture creates potential predicaments for the affected company that needs careful management. While the litigation exposure is hard to measure *ex ante*, the injury from lost customers and/or altered terms and conditions is far easier to measure. An accurate measurement of the injury from lost customers or reduced business from existing customers is critical to support insurance claims for injury from a cyberbreach. These claims flow from decisions by customers and suppliers to discontinue, or alter the terms of, doing business with a breach victim. Any claim can be made; what matters is getting it paid and that depends on what losses can be proved. Developing the requisite proof requires an economic or other financial expert who can dissect market- and firm-specific events, use appropriate statistical and analytical techniques and isolate the economic losses attributable to the breach. The insurance claim is a de facto damages analysis; much as a litigant would not assert damages in court without an expert, asserting a claim for losses due to a cyberevent without expert supporting analysis is a recipe for denied claims.

However, if that injury is deemed *material*, there may be disclosure obligations. At a minimum, those losses could support a claim for damages against the company in a derivative case or support a materiality argument in a stock-drop case. In that case, the cybervictim is better served by knowing exactly what injury it can demonstrate and make an assessment of the impact that is grounded in fact and not wishful thinking or assertion. Indeed, rather than being in conflict with one another, this impact analysis and disclosure obligations actually go hand in hand.

No organization wants to deal with a cyberevent. However, when one occurs, proactively dealing with the issues that arise from a cyberevent gives the cybervictim the best chance of minimizing short- and long-term injury and costs.

Steven Schwartz, an economist, is a vice president with Charles River Associates. He has extensive expertise in commercial damages estimation. The views expressed are his own and do not reflect or represent the views of Charles River Associates or any organization with which he is affiliated.

Reprinted with permission from the March 2018 edition of CORPORATE COUNSEL © 2018 ALM Media Properties, LLC. This article appears online only. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 016-03-18-06