threatSHIELD Security

SEVEN HIDDEN COSTS OF A CYBERATTACK

BY: DELOITTE

There are many ways a cyberattack can affect—and cost—an organization, and the impacts will vary depending on the nature and severity of the event.

Common perceptions, however, are mostly shaped by what companies are required to report publicly—primarily theft of personally identifiable information (PII), payment data, and personal health information (PHI). Discussions tend to focus on costs related to customer notification, credit monitoring, and the possibility of legal judgments or regulatory penalties. And thanks to important work done in this area, the industry is generally converging on the calculation of a "cost per record" for consumer data breaches.

Rarely brought into full view, however, are cases of intellectual property (IP) theft, espionage, data destruction, attacks on core operations, or attempts to disable critical infrastructure. Beneath the surface, these attacks can have a much more significant impact on organizations and lead to additional costs that are both more difficult to quantify and often hidden from public view. A new Deloitte Advisory study, *"Beneath the surface of a cyberattack: A deeper look at business impacts,"* recently outlined the depth and duration of cyber incidents in financial terms.[2] In this issue of CFO Insights, we'll focus on seven costs that are not so apparent and why it is important to include them in calculating the total cost of a cyberattack.

By: Deloitte

BELOW THE SURFACE COSTS

Overall, the cyber report identified 14 business impacts of a cyber incident as they play out over a five-year incident response process—seven direct and seven hidden costs. For the intangible costs, various financial modeling techniques were used to estimate the damage (see “Assigning value to intangible losses”). And the research showed that the direct costs commonly associated with data breaches were far less significant than the “hidden” costs. In fact, in Deloitte’s scenarios, they accounted for less than 5 percent of the total business impact.

Given that impact, CFOs should be aware of the following seven hidden costs:

- Insurance premium increases. Insurance premium increases are the additional costs an insured entity might incur to purchase or renew cyber risk insurance policies following a cyber incident. There is little public data available on actual premium increases following cyberattacks. Deloitte conducted informal research among leading providers of cyber insurance and found that it is not uncommon for a policyholder to face a 200 percent increase in premiums for the same coverage, or possibly even be denied coverage until stringent conditions are met following a cyber incident.* According to our sources, factors that influence future costs may include: a willingness and depth of information provided by the policyholder upon review of the incident; the policyholder’s plans to improve incident handling or other aspects of its security program; anticipated litigation; and assumptions concerning the company’s level of cybersecurity “maturity.”

- Increased cost to raise debt. Increased cost to raise debt occurs when, as a result of a drop in credit rating, the victim organization faces higher interest rates for borrowed capital, either when raising debt or when renegotiating existing debt. Organizations appear to be perceived as higher-risk borrowers during the months following a cyber incident. Deloitte analyzed the credit rating of nine public companies (from the same industry and comparable in size) and observed an average Standard & Poor’s credit rating of A, and assessed these companies against companies that had recently suffered a cyber incident. It was observed that, in the short term, the credit-rating agencies typically downgrade by one level companies that have experienced a cyber incident.

By: Deloitte

- Operational disruption or destruction. The Impact of operational disruption or destruction is a highly variable cost category that includes losses tied to manipulation or alteration of normal business operations and costs associated with rebuilding operational capabilities. This could include the need to repair equipment and facilities, build temporary infrastructure, divert resources from one part of the business to another, or increase current resources to support alternative business operations to replace the function of systems that have been temporarily shut down. It could also include losses associated with the inability to deliver goods or services. The nature of operational disruption—and therefore the appropriate method of calculating its impact—is very specific to each situation and requires direct knowledge of a number of distinct information components.

- Lost value of customer relationships. During an initial period immediately following a breach, it can be hard to track and quantify how many customers are lost. Economists and marketing teams approach this challenge by attaching a "value" to each customer or member to quantify how much the business must invest to acquire that customer or member. They then look at the likely revenue that this one customer or member will generate for the business over time. These numbers can then be evaluated per industry and particular organization to estimate how much investment is needed to attract and acquire new customers.

- Value of lost contract revenue. Value of lost contract revenue includes revenue and ultimate income loss, as well as lost future opportunity associated with contracts that are terminated as a result of a cyber incident. To determine the financial impact of the lost contracts or premiums, Deloitte estimated the value of the contracts in test cases both before and after the cyberattack was assessed. Following a cyberattack, if the subject company were to lose contracts, it was assumed there would be a decrease in revenues. Then the present value (meaning an estimate of the value of a future income stream depicted in present dollar terms; receiving a dollar today is worth more than receiving a dollar in the future, since one could earn interest on that dollar) of cash flows that the company would earn over the term of the contracts was determined.

- Devaluation of trade name. Devaluation of trade name is an intangible cost category referring to the loss in value of the names, marks, or symbols an organization uses to distinguish its products and services. A brand name is associated with the name of a specific company or a specific product, whereas a trade name relates to an organization as a whole. To determine the financial impact of a cyber incident on the value of a company's trade name, the likely value of the trade name both before and after the cyber incident has to be assessed. To value the trade name itself, Deloitte employed the relief-from-royalty method.

By: Deloitte

The relief-from-royalty method, commonly used to value IP assets such as trade names, estimates the value by analyzing what another entity would have to pay to license the company's trade name. Deloitte's analysis involved establishing a reasonable "royalty fee" by looking at royalty fees or rates paid in actual royalty transactions for similar types of IP, and the analysis of profit margins across the industries to which the text cases belong, to determine what a typical company in the industry would have the capacity to pay.

- Loss of intellectual property. Loss of IP is an intangible cost associated with loss of exclusive control over trade secrets, copyrights, investment plans, and other proprietary and confidential information that can lead to loss of competitive advantage, loss of revenue, and lasting and potentially irreparable economic damage to the company. Types of IP include, but are not limited to, patents, designs, copyrights, trademarks, and trade secrets. Unlike other types of IP, trade secrets are protected indefinitely until publicly disclosed. Similar to the value of a trade name, the value of IP is estimated by approximating how much another party would pay to license that IP.

A FULLER COST PICTURE

For all the attention major breaches receive, business leaders, including CFOs, rarely see what occurs behind the walls of an organization struggling to recover from an attack—until it happens to them. Moreover, while cyber incidents may begin as a technology issue, they typically extend well beyond the technology domain and hit at the very heart of business value and performance.

To understand the less obvious impacts of a cyberattack requires a multidisciplinary approach that integrates deep knowledge of cyber incidents with business context, valuation techniques, and financial quantification. But with better visibility into a broader range of the potential business impacts—including the seven outlined here—leaders can transform the way they manage cyber risk and improve their ability to recover when a cyberattack occurs.

ASSIGNING VALUE TO INTANGIBLE LOSSES

Various financial modeling techniques were used to estimate the value of lost IP, damage to trade name, and impact of lost customer relationships and contracts. The following concepts are useful in understanding these methods.

- Valuation and financial quantification are associated with a specific point in time. Given the time value of money and a wide range of unforeseen internal and external factors that may also impact the future value of an asset, the aim of the valuation process is to assign an estimated value or financial benefit to an asset at a specific point in time—in this case, the time the cyberattack was discovered. The study applied the widely accepted Discounted Cash Flow Method under the Income Approach, which broadly entails estimating the present value of the projected economic benefits to be derived from the use of the asset.

- With-and-without method. The "with-and-without" method is a comparative business valuation technique that involves estimating the value of an asset under two scenarios: one, with a certain asset or situation in place (the "situation," in this context, being the occurrence of a cyberattack); and the other without the asset or situation in place (in this case, the absence of a cyberattack). The difference in these value estimates yields the isolated value impact that can be attributed to the situation.

- Reliance on assumptions. Performing a valuation or damages/loss exercise often requires the use of professional judgment and reasonable assumptions in the absence of detailed, actual data. In the study's analysis of the impact of a cyber incident on particular assets in the hypothetical scenarios, typical industry benchmarks were used (or research conducted to identify benchmarks) to arrive at assumptions for a financial impact analysis. Some of these assumptions leveraged Deloitte's experience performing valuations and damages analyses in similar contexts.