Luxury Daily®

The News and Intelligence You Need on Luxury

FINANCIAL SERVICES

Cyber attack damages cost 10-20x more than expected: Deloitte

June 16, 2016

Image courtesy of Bloomingdale's

By FORREST CARDAMENIS

The costs most commonly associated with security compromises amount to less than 5 percent of the business impact, according to Deloitte Advisory.

While the fines, litigation fees and cost to improve cyber security are well-known expenses following a data breach, the loss of intellectual property, increase in insurance premiums and tarnished customer relations often equate to costs of a much higher magnitude. Taking a closer look at the associated costs of cyber attacks can help brands ensure they are properly budgeting security expenditures.

"This report the first accurate picture of the impact of cyberattacks is truly unprecedented," said Emily Mossburg,co-author of the report and resilient practice leader for Deloitte Advisory. Given the picture this provides on the potential impact of a cyberattack to an organization, implementation of a business aligned cyber risk program is critical.

"Our report highlights the need for organizations to focus on securing their environment (including their critical information and data); being vigilant in monitoring for threats and attacks to quickly identify potential incidents; and to be resilient, quickly responding and recovering in the face of attack," she said. "The 14 impact factors identified include those things that are well known and frequently discussed (such as technical investigation, customer breach notification, and legal fees) but also includes those financial valuation elements that to date have not been part of the dialogue (devaluation of trade name, loss of intellectual property and lost value of customer relationships)."

"Beneath the surface of a cyber attack: A deeper look at business impacts" is a risk-based report outlining the duration and lasting impact security compromises have on businesses in financial terms.

Cyber defenses

With information regarding the impact of such attacks being so opaque, Deloitte hopes to paint a clearer picture to help executives better understand what is at stake and how to protect their organization. To begin, the report identifies 14 business impacts of a cyber incident, half of which are more obscure.

The well-known costs are customer breach notifications, post-breach customer protection, regulatory compliance/fines, public relations/crisis communications, attorney fees and litigation, cyber security improvements and technical investigations.

Hidden costs include increases to insurance premiums, increased costs to raise debt, operational disruption/destruction, lost value of customer relationships, lost contract revenue, the devaluation of the trade name and the loss of intellectual property.

These hidden costs regularly equate to at least 20 times the more visible costs. That means that businesses may be improperly budgeting cyber-security, as their calculation of the ratio of the budget for security and potential cost in the incidence of a cyber attack is far removed from reality.

Relatedly, a data breach is not something that incurs a flurry of spending to fix it and can then be forgotten; the costs are prolonged, with initial costs representing around 10 percent of the total cost over five years.

Businesses are beginning to see cyber attacks as a likely occurrence, if not an inevitability, leading many to develop an approach that balances security investments with quick-response and threat-visibility. Nevertheless, improper valuations of cyber attacks make it difficult for organizations to properly prepare, budget and anticipate expenses.

The report details a cyber attack and impending costs of two separate businesses, one a U.S.-based health insurer, the other a U.S. technology manufacturer. Examining these scenarios, Deloitte illustrates how responses, attack objectives and differing industries impact the damage of a cyber attack, but that impact extends further than generally considered.

Going forward, Deloitte recommends clear crisis plans that account for what the breach is and when it occurs in relation to what the business is currently doing. For example, responses should be different when soliciting subscribers or offering an open enrollment because the compromised information should be expected to differ situationally.

Proactively approaching customers whose data may not have been breached is also recommended over hoping news of the attack does not go public. Withholding that information generally only accounts for a small portion of above-the-surface costs, and the minor potential benefits are severely overpowered by the more likely scenario of the breach being made in public and the subsequent bad publicity.

Security outlook
Security breaches are becoming more common, and brands are taking notice.

As digital channels become increasingly important for retailers' businesses, cyber security has jumped to the top of industry insiders' lists of concerns.

A report from BDO finds that 100 percent of retailers cite privacy concerns from a security breach as a worry, up from 55 percent in 2011. With highly publicized cases of hackers successfully sticking their hands in retailers' client data, the possibility of a potential break in security seems more realistic (see story).

Brand across sectors are worried about cyber security, with luxury hotels being recent victims.

Starwood Hotels & Resorts announced last November that a small number of its North American properties were infected with malware.

With its point of sale systems compromised by the malware, unauthorized parties had access to credit card data of some of Starwood's guests. Data infringements unfortunately have become common, but a timely response from brands victimized by these actions can quell consumers' concerns (see story).

"The above-the-surface and below-the-surface costs may all vary greatly based on industry sector, organization and specific incident," Ms. Mossburg said. "Important key considerations driving the impact and cost include but are not limited to, motivation of the attacker, sophistication of attack, how quickly the attack is identified and response is initiated, the environment impacted, and the type and volume of data impacted (e.g. personal information, intellectual property, strategic corporate plans).

"In considering risks specific to retail, for example, attacks often focus on theft of credit card data that may be used to perpetrate financial fraud and identity theft," she said. "This may lead to impacts focused on the loss of personally identifiable information above-the-surface and may include things like lost value of customer relationships and value of lost revenue below-the-surface.

"When considering risks to automakers, you start to get into a number of potential scenarios including targeted attack focused on stealing intellectual property; an attack focused on compromise of a connected vehicle; or an attack focused on disrupting the manufacturing process and vehicle production. Each of those scenarios, would

bring with it a different profile for the quantification of the above-the-surface and below-the-surface impacts."