The cost of a data breach

Like an iceberg, the true cost of a data breach may be far greater than what is immediately visible. If the breach affects regulated data such as personally identifiable information, the organization is obligated to disclose it, leading to public relations and legal costs as it works to repair its reputation. However, what may be far more costly are breaches below the waterline — cyber attacks targeting research and development, intellectual property, pricing and strategy, which are not typically disclosed. The average cost of dealing with a cyber attack was $15 million for U.S. companies in 2015, according to research from the Ponemon Institute. Bottom line? Long term, the cost of improving cybersecurity and privacy practices may seem small by comparison.

Types of costs

External advisors
Following a breach, companies may need to hire investigators, data privacy attorneys, specialists in notifications and credit monitoring experts to help address the crisis. Publicly disclosed breaches will also incur public relations costs to mitigate reputational damage.

Undisclosed breaches
Businesses are not obligated to report breaches of intellectual property data such as product designs (SEC guidance exists but it does not require detailed disclosures). However, the potential losses could be far greater if billions of dollars’ worth of research or intellectual property is stolen by a rival or a nation state.

Third-party breaches
Trusted insiders were responsible for 43% of data loss incidents, according to 2015 research by Intel1, half of which were accidental and the other half deliberate. Companies must ensure data security policies apply just as stringently to internal processes as to access from external systems.

Publicly disclosed breaches
Companies are obliged to report breaches of sensitive personal data, such as credit card information and protected health information.

Containment and remediation
When a breach occurs, companies will incur the cost of restoring the network and rebuilding it to better prevent a similar breach from occurring. Post-breach, organizations often transform their cyber threat monitoring and increase security personnel in order to detect future attacks at earlier stages.

Executive displacement
Following some high-profile breaches, CEOs have been removed from their posts. Firing and replacing senior management causes disruption and incurs costs related to severance and recruitment.

Competitive erosion
If sensitive corporate information – research and development data, merger and acquisition details, pricing and time-to-market information – is revealed via a breach or other occurrence, long-term damage, diminished stature and erosion of value can result. Breached companies may face new legal costs; people whose personal data was affected may bring a class action suit; shareholder action may result if the stock price was affected; and there could be regulatory inquiries, depending on the industry.

Lost revenue and market share
A breach can have an immediate impact on a company’s bottom line. For example, when a large retailer’s credit card information was breached, the retailer experienced a noticeable dip in quarterly profits before the breach was made public. However, the impact of intellectual property theft to the bottom line can be far greater: for companies that have spent billions of dollars on research and development, the loss of unique designs, systems and strategies may trigger a sudden drop in market position.

Breach investigation
Hiring forensic experts to thoroughly investigate how systems were breached and what was accessed can be costly. Time is of the essence to do so, given the unforeseen consequences such as litigation and regulatory requirements. Creating a timeline of events enables an organization to maintain an accurate picture of what happened long after the breach.

Types of loss

Breach investigation
Executive displacement
Competitive erosion
Lost revenue and market share


© 2017 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.