

14.3.2 Consequences of Breaches Facts

Network and data breaches can have serious consequences. Some of them can be far reaching and potentially permanent.

This lesson covers the topic of the consequences of breaches:

Consequences of Breaches

Breaches affect all companies. This includes even large companies with security budgets in the millions of dollars. Most of us have, at one time or another, been notified that our information has been compromised. It could be bank accounts, credit cards, government records, or even health records. All these data breaches come with serious consequences.

Category	Description
Reputation damage	<p>A company's reputation determines if people invest, if consumers buy a product or service, or if foreign governments even allow a certain company to do business in their jurisdiction. A company lives or dies by its revenues and investments, so a breach that exposes client data directly affects the way consumers and investors spend their money. A data breach can cause stock prices to fall, and falling stock prices lead to sell-offs and permanent damage.</p> <p>Consumer confidence is damaged and trust broken when a breach occurs. Revenue drops because consumers stop using the company. This doesn't include any government contracts a company may have, the loss of which can prove fatal.</p>
Identity theft	<p>Twenty years ago this term didn't have any real meaning to the everyday person. Fast forward to today and it is difficult to find someone who hasn't experienced identity theft on some level. When a breach occurs and personal information is stolen, the affected person is forced to do hours of work to correct someone else's mistake.</p> <p>The effects of identity theft can last for years and cause fear and paranoia among the victims. Lives have been turned upside down, leaving victims frustrated because it is almost impossible to catch the perpetrator.</p>
Fines	<p>A data breach can also be financially costly. Now, with the introduction of GDPR and the California Consumer Privacy Act, the number of companies that can be fined has grown significantly. In the United States, HIPPA has always carried fines for companies found in non-compliance.</p> <p>Companies that profit from the use of personal information can also have heavy fines levied against them by the Federal Trade Commission and possibly the Security and Exchange Commission. To give you an idea of the magnitude of these fines, three data breaches at three separate companies cost the companies over one billion dollars in 2019. It is estimated that a single data breach now averages \$6.45 million dollars.</p>
IP theft	<p>Intellectual property (IP) is the lifeblood of companies. When their IP is stolen, they lose competitive advantage. The internet has made the world smaller, and companies are now competing with others from around the globe.</p> <p>When IP is stolen through a data breach, it is often sold to competing companies. Many of the companies are overseas and not subject to laws in the United States, making them</p>

	<p>difficult to prosecute. This allows the reverse engineering or direct copy of IP and gives the thieves an undeserved revenue source. This also floods the market with counterfeit goods.</p>
Notifications	<p>Each of the 50 states now have laws on breach notifications. Most of the laws have common elements. For example, a company must immediately disclose a breach to its customers in writing.</p> <p>There are, however, exceptions to this. If a company determines, after a good-faith investigation, that the breach is unlikely to lead to the misuse of personal information, notification is not required. Most companies do notify the public when a breach occurs to prevent loss of public trust.</p>
Escalation	<p>Escalation can be separated into two categories, which are internal escalation and external escalation. Internal escalation is part of a company's incident-response plan. This usually means a tiered approach to informing management of a breach. As a breach is investigated, the findings and severity determine how far the escalation goes.</p> <p>External escalation is when experts need to be brought in from the outside to investigate, provide legal counsel, or even enforce laws. The key is to know when a situation has surpassed your ability to resolve it.</p>

Copyright © 2022 TestOut Corporation All rights reserved.