Report on Supply Chain Compliance Volume 2, Number 13. July 18, 2019
The risk of a data breach to your supply chain is real … and so are the solutions

By Sascha Matuszak

The United Kingdom's Information Commissioner's Office announced its intention to levy two separate fines, including the largest yet under the GDPR, on consecutive days in July. The intended fine against British Airways, announced on July 8, would be GBP 183.39 million (more than USD 230 million), while the fine against Marriot International, Inc. would be GBP 99.2 million (more than USD 124 million).

"People's personal data is just that – personal," said Information Commissioner Elizabeth Denham. "When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."

The fines — especially the fine against British Airways — are intended to be a collective message to organizations that handle European data: Be serious about security, or you will be punished.

Data breaches are extremely common, and hackers tend to view corporations as the soft underbelly of a nation. Estimates place the number of hackers (primarily state actors) actively pursuing economic targets across the globe in the hundreds of thousands. In contrast, most corporations have, at most, a few dozen employees working on security and information technology systems management. Billions of U.S. dollars are lost each year to cyber espionage, and hundreds of millions of individuals' personal data has been compromised and exploited for economic or political gain. Cybercrime that results in financial damage is also on the rise, and hackers that find themselves underpaid by their state employees are selling their services on the free market or joining together in "composite groups" to attack and exploit vulnerable systems.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login