

CASE STUDY

Nonprofit Faces Data Privacy Fallout Following Widespread Software Breach



INDUSTRY

Nonprofit

EVENT TYPE

Data Breach

REVENUE

\$50–100M

EMPLOYEE COUNT

51–250

LOCATION

Washington, D.C.

KEY COVERAGE

Breach Response

An international nonprofit organization was one of the thousands of organizations impacted by a zero-day vulnerability in a popular file-transfer tool. More than 600 unique files related to individuals from the United Kingdom, United States, Canada, Australia, Germany, and the Netherlands were exfiltrated in the event. Due to concerns about legal obligations and other regulatory requirements, the nonprofit contacted Coalition for assistance.

Coalition Incident Response¹ (CIR) quickly launched a forensics investigation to review the extent of the event, as the compromised data included donor names, addresses, credit card numbers, phone numbers, email addresses, and bank account details. At the same time, we established breach counsel in each impacted region to review regulations and affected data.

CIR determined that the threat actor’s activity was limited to the server running the file-transfer software and found no evidence of lateral movement or additional malicious software on other systems. CIR’s findings were also consistent with other organizations impacted by the zero-day vulnerability and didn’t require extensive restoration on the nonprofit’s end. Here’s how one key coverage responded to this data breach: Breach Response² covered the cost of numerous local breach counsels and a full forensic investigation. After the nonprofit paid its \$25,000 self-insured retention, its policy covered more than \$35,000 in costs related to the claim.

» International Businesses Face Increased Scrutiny Over Data Privacy

When data is shared across jurisdictions, it can be subject to different data privacy regulations. International businesses that operate in many regions typically face increased scrutiny over their data privacy practices. While the expectation is that businesses are always in compliance with applicable local regulations, they should also anticipate additional costs when it comes to responding to a cyber event, like a data breach.

Coalition brings together active monitoring, incident response, and comprehensive cyber insurance designed to help mitigate your organization’s cyber risk. To learn more, visit coalitioninc.com.

¹ Coalition Incident Response services provided through Coalition’s affiliate are offered to policyholders as an option via our incident response firm panel.

² The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

International businesses that operate in many regions typically face increased scrutiny over their data privacy practices.