

How a Global Manufacturer Beat a Ransom Deadline—and Refused to Pay



SUMMARY

When a global manufacturing organization was targeted in a ransomware attack, its leadership faced a decision under extraordinary pressure. The threat actor claimed to have stolen approximately 1.3 terabytes of enterprise data from 21 internal servers and issued a five-day ultimatum: pay the ransom or risk public disclosure of the stolen information.

For an organization operating across more than 40 countries, the consequences extended beyond the immediate disruption. The compromised dataset potentially contained employee information, financial records, and other sensitive data subject to multiple privacy and notification requirements. Without knowing precisely what had been taken, executives faced the prospect of making a ransom decision without a reliable understanding of the organization's exposure.

ACTFORE was engaged alongside outside counsel to change that equation. Rather than limiting the engagement to an initial assessment of potentially sensitive files, the objective was to determine what information was involved, identify the affected individuals, and produce a complete notification list before the threat actor's deadline.

In just four days, ACTFORE completed the analysis and delivered the notification list—one day before the five-day ultimatum expired. Armed with those findings and a defined path toward notification, the organization's executive leadership refused the ransom demand. The engagement demonstrated how rapid, comprehensive data analysis can do more than support post-incident notification. When performed early enough, it can provide critical intelligence for the ransom decision itself.

RESULTS

1.3 TB
Data involved in the incident

900K
Files analyzed

4 Days
Complete notification list delivered

CUSTOMER DETAILS

- Industrial Manufacturing
- Global Operations
- Motion & Control Technologies
- COUNSEL
 - Am Law 100
 - Chambers Ranked

PRODUCTS USED

- BOXER
- CLARITY
- IMPACT-IQ
- DISCOVER
- TRACE

FIVE DAYS TO MAKE A DECISION

The cost of not knowing what was taken

The ransomware attack placed the organization in a difficult position. The threat actor's demand created an immediate financial decision, but the consequences of that decision depended in part on information leadership did not yet possess: the nature and extent of the sensitive data exposed.

Paying the ransom would not necessarily guarantee deletion of the stolen information or eliminate potential notification obligations. Refusing payment, however, required leadership to understand the potential consequences of disclosure and prepare for the regulatory and operational response that could follow.

For a multinational manufacturer, the analytical challenge was substantial. Approximately 900,000 files required examination across a dataset containing information associated with international operations. The analysis needed to identify 17 critical data elements, including national identification numbers, health insurance information, and financial records.

Under conventional review timelines, establishing individual-level exposure could take weeks. The threat actor had given the organization five days.

Turning an ultimatum into an analytical deadline

ACTFORE's role was to provide more than an estimate of potential exposure. The engagement required a complete progression from identifying sensitive files to extracting relevant information, associating records with affected individuals, and preparing a notification list suitable for counsel's use.

This distinction mattered to the executive team. A preliminary estimate might indicate how serious the incident could become, but it would not provide the same degree of clarity as a completed assessment of affected individuals and associated data.

The objective was therefore unusually direct: deliver the information necessary to support the organization's response before the threat actor's deadline expired.



I have sent very complex datasets to Actfore. They were able to analyse without any complications and ahead of schedule.

Client
Chambers | Crisis & Risk Management 2025

FROM RANSOM UNCERTAINTY TO AN INFORMED DECISION

Establishing the scope of exposure

ACTFORE deployed its AI-powered data mining technology to begin analyzing the compromised dataset immediately. Within the first 24 hours, the platform had identified patterns associated with 17 critical data elements, providing early visibility into the types of sensitive information present.

The analysis progressed beyond file-level identification to the extraction and consolidation of individual-level information. Automated processing enabled the team to examine large volumes of heterogeneous enterprise records while concentrating review and validation efforts on findings relevant to the organization's potential notification obligations.

The engagement ultimately identified more than 206,000 files containing sensitive information associated with approximately 120,000 individuals. These findings provided a concrete understanding of potential exposure that could be evaluated by outside counsel.

Completing notification analysis before the ransom deadline

Four days after engagement, ACTFORE delivered the complete notification list. The organization now had the information needed to understand the identified affected population and the sensitive data associated with those individuals, before the threat actor's original five-day deadline.

This changed the circumstances under which the executive team could evaluate the ransom demand. Rather than making a decision primarily under the uncertainty created by the threat actor's claims, leadership had access to substantive findings and a defined path for managing potential notification obligations.

The executive team refused to pay the ransom.

ACTFORE's analysis did not eliminate the risks associated with stolen information, nor could it guarantee what the threat actor would do next. It did, however, help remove a critical source of uncertainty at the point when leadership needed to make a consequential decision.

The outcome illustrates a broader opportunity in ransomware response: sensitive-data analysis does not always have to wait until the extortion phase has concluded. When completed early enough, the same work required for breach notification can also inform the organization's ransom strategy—without requiring a separate analytical process.

EARLY INTELLIGENCE UNDER PRESSURE

Within the first day, ACTFORE surfaced patterns associated with 17 critical data elements, giving counsel an early indication of the types of sensitive information present while the broader review continued.

24 HRS

Initial sensitive-data patterns identified

FROM EXPOSURE TO NOTIFICATION READINESS

Within four days, ACTFORE identified approximately 120,000 affected individuals and delivered a complete notification list, giving counsel the information needed to prepare for disclosure before the ransom deadline.

120K

Individuals identified for notification



The objective wasn't simply to process the data before the deadline. Leadership needed to know what had been taken and whether the organization was prepared to manage the consequences of disclosure. Delivering the notification list in four days gave them information they could use when making that decision.

Daniel Lim
Co-Founder | VP of Data & Client Solutions
ACTFORE

Don't let a ransom deadline dictate your decisions.
Understand what's been exposed, identify who's affected, and gain the clarity needed to make informed decisions—before time runs out.

CONTACT US