CASE STUDY

A Quick, Effective Resolution to a Phishing Incident

Data Breach Discovery™ helped a medical research company quickly review data and resolve a cybersecurity incident.

Situation

A medical research company experienced a data security incident caused by a phishing email. Although a forensic response team identified and remediated the breach within a few days, several mailboxes were still compromised and accessed by bad actors during that time.

Solution

In consultation with a forensic response team, which reviewed all company emails to identify which ones were affected by the breach, it was determined that six email accounts, containing a total of approximately 30,000 emails and attachments, had been exposed. Using proprietary analytics and searches, the data breach discovery team quickly detected that 10,000 of the exposed documents had potentially private information that would require notification letters to individuals and government agencies.

The set of documents with potentially private information was further assessed, revealing that 2,700 were false hits, thus, eliminating them from requiring further review. The team further discerned that a small handful of spreadsheet files contained several hundred individuals' private data. These files were moved to a discrete automated data extraction workflow for handling. The balance of the document set contained a variety of potential privacy items, which was organized for efficient review and data capture.

Using proprietary analytics and searches, the data breach discovery team quickly detected that 10,000 of the exposed documents had potentially private information that would require notification letters to individuals and government agencies.

Success

Our consultants quickly extracted the affected individuals' information from the spreadsheets. Other resources managed the manual review and data capture of the larger document set. The data breach discovery team deduplicated the resulting list of affected individuals and provided the client with a clean list of individuals requiring notification, as well as a summary of the states and foreign jurisdictions involved.

By combining several key competencies — eDiscovery principles, advanced text analytics, cutting-edge database analysis and a detailed understanding of privacy issues — the team was able to quickly, efficiently and cost-effectively review this large amount of data and resolve the incident. Thanks to in-depth experience and highly tuned workflows, the entire process from ingestion to delivery of the clean notification list was completed in less than four days.

BIA'S MISSION, VISION AND GUIDING PRINCIPLES

Mission:
We strive to exceed our clients' expectations, to never stop learning and innovating and to keep our guiding principles central to everything we do.

Vision:
To solve even the most complex eDiscovery needs with an unrivaled blend of outstanding customer service, talented professionals, innovative technologies and superior workflows.

Guiding Principles:
- Service Excellence – Clients are our #1 priority.
- Client Protection – Defensibility and security are in our DNA.
- Team Collaboration – We build truly effective teams.
- Transformative Solutions – We create order from chaos.
- Industry Leadership – We lead by example.
- Continuous Education – We understand the importance of education.