Morae's Data Breach Response Solution

70B+

Records exposed in breaches (2020)

$8.4M

Average US cost per breach

600%

Increase in cyber crime (2020)

Increasingly complex notification laws at state, federal, and industry levels.

Data Breach Response Challenge

We've all seen the headlines or been personally affected by a cyber event. In today's digital global economy, the problem is rampant.

As part of Incident Response, corporates must consider breach notification laws that require companies to notify customers if their PII/PHI is exposed in a breach.

Hackers are increasingly targeting business emails, chats, and file-shares. This complicates notification.

When a structured database is compromised, the contents drive the notification. But what if the contents are unknown?

Determining the scope and nature of PII/PHI in unstructured data can be time consuming and costly and presents a risk of non-compliance.

In the event of a breach, you need a partner you can trust to quickly and cost effectively tell you which customers PII/PHI has been compromised.

Morae's Solution

Morae's Data Breach Response Solution identifies and reports on customer PII/PHI in unstructured data sets such as emails, chats, or file-shares. We help our clients comply with breach notification mandates.

Our expert team applies an effective process with award-winning technology.

Morae's Cyber Breach Project Managers are experts in workflow, technology, and team oversight. We can scale quickly thanks to a global roster of vetted cyber analysts experienced in breach response.

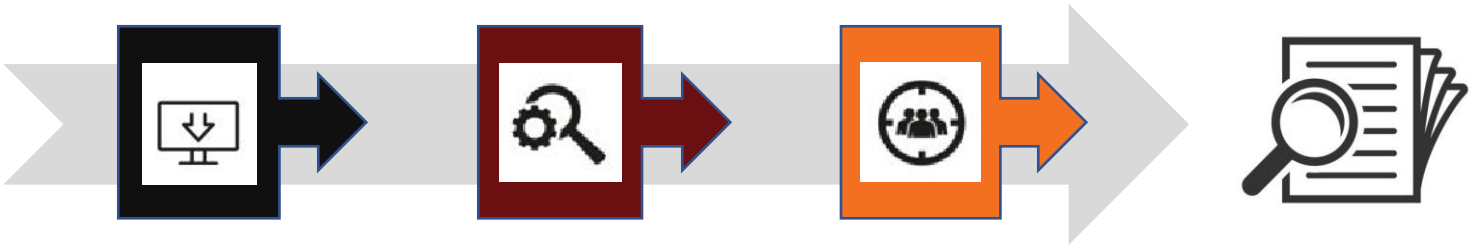
Our well-established Breach Response Playbook applies a rigorous process from start to finish. Our reporting is digestible and actionable.

Morae's technology stack is purpose built to solve this problem. We leverage machine learning to identify PII/PHI and auditable review workflow to validate the output and quickly generate an Entity Notification List.

MoraeCyberBreachTeam@moraeglobal.com

Morae's Data Breach Response Workflow

Our three-step process achieves actionable intelligence



Prepare

Forensic best practices to collect data that requires analysis from any medium.

A Day One Kickoff call asks the key questions across the end-to-end process with all stakeholders.

Analyze

Machine learning and rule-based algorithms identify and tag dozens of PII/PHI elements in processing.

Our Impact Assessment Report tells you scope and nature of PII/PHI as soon as the data is in our platform

Validate

Deep bench of experienced cyber reviewers validate the auto-tagging to link customers with their PII/PHI.

Clear reporting keeps you informed on progress and trends.

Comply

Our technology is purpose-built to efficiently create a deduplicated entity notification list.

Note, we further support investigations or litigation resulting from cyber events.

Advantages of Morae's Approach

Team

- Project managers are experts in managing the end-to-end process
- 1000s of cyber analysts available on demand
- Onshore & offshore capabilities

Speed

- Established Playbook advances your objectives beginning in a Day One Kickoff
- An Initial Impact Assessment tells you what PII/PHI exists as soon as data is processed

Value

- Better PII/PHI identification technology means fewer documents to review
- Faster review pace than traditional discovery platforms
- Less time to create a notification list

Comprehensive

- End-to-end Incident Response coverage with our partner network
- Experts from start to finish in data and analysis for cyber review

moraeglobal.com

MoraeCyberBreachTeam@moraeglobal.com