Data Protection Priorities Assessment

CHALLENGE

In response to the California Consumer Privacy Act (CCPA), a subsidiary of a Fortune 500 global investment and advisory financial services firm needed to conduct a data protection priorities assessment of procedures and practices that impacted consumer policies data. The assessment included reviewing, documenting, and mapping its data process workflows, security procedures, and other practices to protect its consumer data.

PROBLEM

- Policyholders' personally identifiable information (PII) was stored, reported, or transferred between eleven (11) potential IT applications, interfaces, datastores, and reports.
- Field names in the company database application did not match the paper or electronic versions.
- The field name differences between sources required analyzing the actual data and where it is placed within the application.
- To provide a direct match back to the client application, relationships, codes, and field values needed to be identified.

SOLUTION

The netlogx team utilized one of our technical data analysts to gain access to the actual technical source code used to create reports to determine data sources on each of the reports. In so doing, netlogx consultants:

- Identified and mapped linkages, data extracts, and data transfers of the seven ancillary systems that store and transfer PII data throughout the organization.
- Built a comprehensive worksheet of what and where each identified PII data element was stored within the various systems.
- Developed a consumer application intake workflow.
- Developed a master tracking spreadsheet with real-time access for the IT department.

ADVANTAGES

The netlogx team of subject matter experts was able to quickly identify and document where the client's customer's personal data is stored. This knowledge was critical for the client in terms of accurately responding to client customer„s request for this information based on the CCPA rules. Failure to do so could result in penalties for the client.

RESULT

The client now has a consolidated repository to know where all of its PII data is stored, moved, and identified. This knowledge has given this company the ability to comply with the required personal data access requests from California policy holders as well as proactively anticipating more state and federal data privacy regulations.

Throughout the Data Protection Priorities Assessment, the netlogx team identified PII vulnerable data in-transit. Our findings are helpful to determine future security encryption needs to protect this PII data. This information serves as a baseline to document and develop a more robust security environment to secure this PII now and in the future.