Case Study

Financial Services Data Security Supports FTC Requirements and Improves Customer Satisfaction

Client Profile

A multinational financial services corporation headquartered in New York City, the client operates in 42 countries with more than 1,300 offices and 60,000 employees globally.

Since 2009, the client has relied on Essintial for End-User and Data Security Services, now supporting 57,000 desk side personal computers in the US with onsite hardware repair services. With a focus on data security, the support agreement has led to a data management program providing hard drive shredding services, destruction, and disposal.

The Challenge

Customary of financial institutions, the financial planning division is responsible for the secure collection and maintenance of customers' personal information including bank and credit card account numbers, income and credit histories and Social Security Numbers.

The FTC (Federal Trade Commission) Safeguards Rule requires companies to assess and address risks to customer information of all operational areas, including three areas pertinent to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures. To meet the FTC tracking and reporting requirements, Essintial created a manageable chain of custody process and tools to capture, collect, and report hardware attributes.

Essintial PPS (Printer and Personal Systems) and Data Security Solutions

- Nationwide 24x7x365 data management
- Data security for 1,200+ service events annually
- Continuous hard drive shredding services
- Sensitive customer data protection
- Chain of custody for memory resident devices
- Exceed service level objectives
- Mitigate risk by leveraging data security best practices

The Solution

Essintial designed and developed a complex data management program and related processes to secure and protect sensitive customer data. Those processes and tools helped manifest a robust data security vehicle for FTC guideline and covenant compliance. They were also used by Essintial's Managed WorkForce™ solution for the client's end-user and field repair services through:

- A designated representative who coordinates the client information security program
- Customer information risk identification and assessment in each relevant area of the operation
- Evaluation of the current safeguards' effectiveness of controlling risks
- Design and implementation of a safeguards program which is regularly monitored for compliance
- Program flexibility allowing adjustments to support evolving circumstances, such as changes in the business or operations, the results of security testing and monitoring, or new FTC requirements.

The Value

Now, with Essintial's streamlined end-user and PC break-fix programs fully deployed, the client's data security programs meet all FTC requirements, allowing them to focus on internal data security measures and safeguards. The onsite repair and secured hard drive data destruction and disposal security processes are efficient, and have alleviated the clients' risk of high cost security breaches.

The Results

Essintial continues to successfully provide hundreds of monthly end-user services to the client while adhering to the strict client and Federal data security protection standards implemented. Most importantly, customer data and its security is protected throughout the services lifecycle.