Data Protection Plan – Why is it Important?

No one can guarantee 100% protection against hackers or malicious intent. Organizations should consider the possibility that they can reduce the likelihood and impact of a data breach by having appropriate processes, plans, and measures in place. The effective measures (tools, technologies, processes, and plans) implemented may not prevent an incident like data breach, but they certainly can act as a deterrent and slow down the compromise process. An effective program also allows for immediate notification to the appropriate personnel within the organization who can act swiftly to isolate the incident. To respond timely and appropriately, an organization must have an effective data protection plan in place. Please note the emphasis on “effective.” Many organizations claim to have a strong data protection plan on paper, but those same organizations cannot vouch for the effectiveness of the plan because it was never completely implemented or was not complete and adequate to begin with.

So why is having an effective data protection plan that has been enforced and implemented important? Consider how much time, money, and manpower companies like SONY and CITI will have to expend to recover from their respective recent breaches where substantial number of customers’ data was compromised. Some analysts are predicting the damage will be billions of dollars.

In addition to the above, there are plenty of reasons why a data protection program and plan may be important in today’s IT environment, which is changing at the speed of light:

- Assists in identifying your organization’s data sources, data owners, and, most importantly, who should and should not be using the data
- Forces organizations to classify data – not many organizations do this. If you don’t classify the organization’s data, how do you know which data is sensitive and which is not and what the impact could be should it be compromised
- Helps prioritize the efforts around implementing effective measures to protect the critical and sensitive data. Oftentimes organizations expend time and resources protecting data that may not be significant or critical and forget about the data that could be more vital (this could be a result of lack of data classification)
- Demonstrates due diligence on behalf of management and best practices
- Makes complying with legal and regulatory laws easier and less stressful (GLBA, FISMA, HIPAA, PCI-DSS, Red Flags, etc.)
- Promotes data protection brand internally
- Creates cross-organizational collaboration opportunities and increases awareness amongst employees and business units

Data protection is needed not only to protect the data on your own systems from harmful threats, but also to ensure that if it does find its way into the wrong hands, it remains secure and unable to be viewed. Of course, as with anything else, the willingness of stakeholders and employees to buy into the plan is critical to the success of data protection.