

Data Privacy Best Practices

Case studies and samples of groundbreaking work being done by Axis in Data security

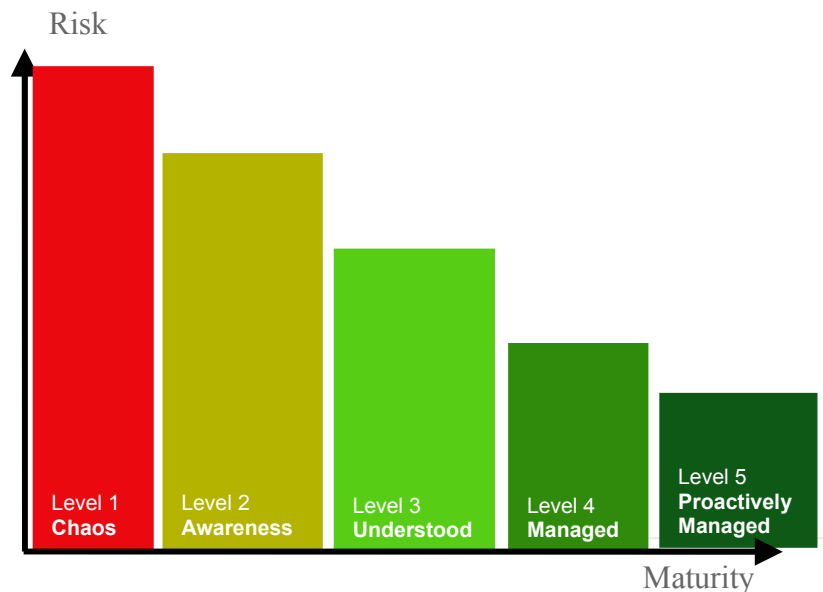
A DATA SECURITY SERIES CASE STUDY

The issue of data privacy can no longer be ignored. The combination of customer outrage around data breaches and new laws and regulations require companies to have a data privacy policy in place or risk significant fines and negative publicity.

Introduction Starting in 2002 with the California data privacy law CA 1386 until recently with the Massachusetts data privacy law MGL 93H, companies are being required to protect customer data and have a data privacy policy in place. Inefficient or non-existent Data Privacy programs result in inconsistent, incomplete and overlapping use of resources (people, process, and tools) to meet data privacy objectives. The first step to address this is to establish or update your data privacy policy based on industry best practices.

1 Data Privacy Maturity Model

A maturity model aids in objectively defining, understanding and assessing sensitive data security. Used as a guide to higher levels of quality, the maturity model can lead to far-reaching improvements in the efficiency and effectiveness of the data privacy program. The diagram to the right illustrates how risk substantially decreases as the data security program, policy, and controls mature.



2 Efficiency & Effectiveness and the Maturity Model

Used as a guide to higher levels of quality, the maturity model can lead to far-reaching improvements in the efficiency and effectiveness of the data security program.

Level 1 – Data Chaos

- There is no sensitive data policy, limited knowledge about its whereabouts, and how to protect it

Level 2 – Data Awareness

- The people, processes and tools used to protect sensitive data are evolving. These are reactionary and produce unpredictable results.
- One-off initiatives have begun to inventory and mask data. Scripts have been written.

Level 3 – Data Understood

- The enterprise has formalized and disseminated a data privacy policy in response to a heightened awareness of potential risks and the efficiency benefits.
- The organizations, processes, training, and tools needed for protecting sensitive data are based on the policy

Level 4 – Data Managed

- Processes are in place to monitor access to sensitive data to detect inappropriate access.
- Tools for inventorying, masking, provisioning, monitoring, and auditing sensitive data are uniformly used across the enterprise and consistently produce high quality results.

Level 5 – Data Proactively Managed

- User provisioning automatically provides entitlements to sensitive data for those users with a need to know.
- Monitored databases provide automatic logging and alerts to the ISO of breaches to this policy.



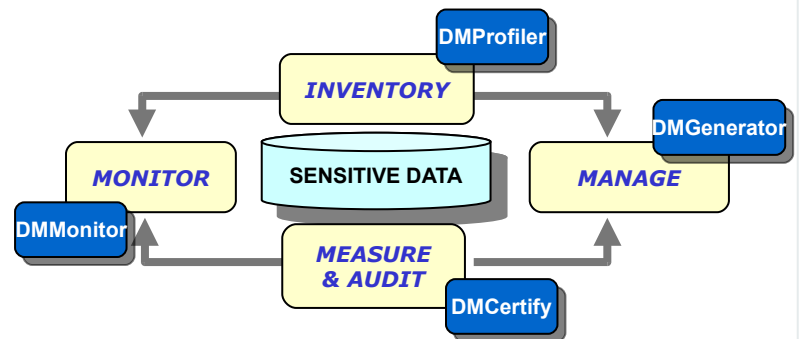
3

Data Privacy Processes

A privacy policy is based on the principle that sensitive data needs to be identified, monitored, managed, and audited. Experience has shown that a process perspective is extremely important to improve efficiency and will result in a consolidated privacy policy integrated across your enterprise. The use of one or more tools in conjunction with your data privacy policy will help institutionalize it and ensure access appropriate to role is enforced.

Axis DMSuite™ enables standardization on a single toolset as an important step in process improvement:

- the suite can manage data on any platform
- the tools are designed to support your data security policy process not force your policy to follow the tool



4 Entitlements, Encryption, Third Parties, Transmissions and Developer Access

A complete data privacy policy needs to cover all the areas where data is shared. Consistent policies need to be designed and enforced in a reasonable manner. A determination needs to be made about what data a person needs to do their job. The default approach should be that a person does not have access to data or systems without explicitly being granted access. Tools already exist to manage access to the resources mentioned here, however the data privacy policy needs to clearly state how and when these tools should be used.

- The data privacy policy must be clear, unambiguous and address both external and internal risks
- A process to identify and manage sensitive data data needs to be defined
- The data privacy process needs to be supported by the use of efficient tools
- Unguarded entry points between lines of business need to be secured
- Encryption is not enough!
- Users should only have access to the data they need to do their jobs
- A process to handle exceptions should be defined

5 Conclusion

Inefficient Data Privacy programs lack cohesiveness, consistency and integration. They can have unpredictable results and therefore uncomfortable levels of data privacy risk. A maturity model aids in objectively defining, understanding and assessing sensitive data security. When used as a guide, it leads to reduced risk and improved efficiency and effectiveness:

- A process approach to data privacy leads to improved efficiency through consolidation and integration
- DMSuite™ provides the tools needed in growing and maturing the PHI data security program

In Closing

A maturity model is useful in determining what you need to do to establish a working data privacy policy. The combination of a clearly defined process and efficient tools will allow you to institutionalize your data privacy policy. This, in turn, will reduce the risk to your business of a data breach which could have far reaching consequences.

Data privacy policies are no longer optional, in fact they are required by many states for larger companies. A customer trusts a vendor will manage his personal data in a professional and conscientious way. If this trust is broken customers will respond by taking their business elsewhere.