Decilog

Secure Software for Mission-Critical Systems

Industry - Financial Services
Cybersecurity

CASE STUDY

Note: A Decilog affiliate participated in the following project.

Creation of Information Security and Privacy Policy, Standards and Procedures

CHALLENGE

In order to have an effective cyber security program, it is imperative to have a formal set of information security and privacy policy, standards, and procedures. The policy consists of high level statements as to management's expectations for appropriate behavior by employees, contractors, etc. Standards are more specific requirements for implementing policy. Procedures incorporate the tasks and oversight required to implement policy and standards.

APPROACH

A key aspect of generating information security and privacy policy, standards and procedures is having knowledge of the laws and regulations that pertain to specific activities at particular locations. For example, privacy requirements will certainly differ by country and are often different from state to state. It is therefore very necessary to involve senior management and representatives – from Legal and Compliance, Human Resources, Accounting, Operations, Marketing, Sales, and the like – in the development process for policy, standards, and procedures, and to obtain the appropriate sign-offs of the completed documents. It is also important to keep such documents up to date by having periodic reviews and by examining the impact of any material external or internal changes.

The policy and other documents were posted so that they could be accessed by all employees, and presented to contractors and other third parties who might be subject to them. Also, an auditable awareness and training program was introduced so that it could be proven that a particular person had been made aware of the requirements.

BENEFITS

It is often held that security and privacy enforcement must come from the most senior management of the organization, and this was achieved by having all interested parties involved in the process and signing off on the resulting documents. It is key that every security or privacy policy, standard or procedure be published and enforced. Such a formal process generally satisfies auditors and regulators.

RESULTS

The information security and privacy policy, standards and procedures, as part of an overall program, led to a high measure of compliance and a reduction in security incidents and privacy infringements.