

# Data Centric Security

By Kevin Doyle, CISSP, ISSMP,  
CISM

## Introduction

Data is a critical, intangible asset to any organization. Data is stored on paper, electronically, and can also be retained by humans. It flows in many forms as well (electronically, through paper reports, forms, and letters, and by word of mouth). Protecting information assets presents multiple challenges.

## Problem Statement

Traditionally, information security has been a function and responsibility of the Information Technology Department within an organization. The view originates from the view that most information is stored and transmitted through computers and also that the biggest threats were hackers and viruses.

While an effective information security function can be placed in the I.T. Department, the focus of security being solely on the technology is flawed.

More and more regulations are being passed at all levels to protect information and ensure that breaches of personal information are disclosed to affected parties.

Information Security Management is responsible for protecting data critical to the organization's mission from the time it originates to the time of disposition – *the information lifecycle*, regardless of the form of critical data or how it is being transferred.

# Data Centric Security (cont.)

By Kevin Doyle, CISSP, ISSMP, CISM

## Previous Options

The traditional method of information security was to protect critical systems, similar to the approach used for disaster recovery strategies.

Focusing only on a single form of information and or one means of transporting data leads to critical errors or oversights, and eventually to breaches.

This protection strategy starts in the middle – *at the point information is electronically stored* – and not on the entire lifecycle of critical data. It ignores paper forms and reports, the human factor and the means of transferring the information, the outsourcing of data handling to vendors and business partners, etc.

## Reclamere Data Centric Solution

A security strategy should be holistic, centered on protecting critical information assets of the organization. At Reclamere, all services are designed based on this philosophy.

This type of protection focuses not only on the critical systems and technology, but also on the individuals who handle the data, and on all formats information can take (paper, electronic, human, etc.

### Benefit 1

The data centric approach protects against information falling into the wrong hands (confidentiality, privacy); unauthorized or unintentional changes to the data (integrity); and destruction or

# Data Centric Security (cont.)

By Kevin Doyle, CISSP, ISSMP,  
CISM

loss of data (availability). It includes all three points of the information security triad – confidentiality, integrity, and availability.

## Benefit 2

Another benefit of a data centric strategy is that it allows the information security program to be aligned with the mission and the priorities of the enterprise. For financial institutions, the organization's most pressing security need may be to focus on protecting the confidentiality of the financial and non-financial information of its customers or members. For healthcare, government, or educational organizations, the main concern may be the integrity of the data being generated. For storage companies or retail merchants, the priority may be availability. By defining these priorities, organizations are more able to mitigate the risks for specific situations based on the priorities of the organization.

## Benefit 3

A third benefit of the approach is that organizations can better be able to comply with regulations and standards. GLBA, HIPAA, Sarbanes-Oxley, the data breach laws, as well as the PCI standards all have information security implications. In addition, if an entity chooses to comply with best practices such as ITIL, ISO 27001, CobiT, etc., they must protect critical data appropriately. Centering on data allows management to mitigate the noncompliance risk.

## Data Centric Security (cont.)

By Kevin Doyle, CISSP, ISSMP,  
CISM

## Reclamere Data Centric Solution

Reclamere's experts can help you evaluate and help an organization's management to implement a strategy that centers on your critical data. For more information, please contact one of our account representatives.



Kevin Doyle, CISSP, ISSMP, CISM  
Security Audit and Assessment  
Manager