

## To Retain or Not To Retain?



*Kevin Doyle, CISSP,  
ISSMP, CISM*

Security Audit and  
Assessment  
Manager

## That Is The Question

Thanks to the Internet and the Information Technology Age, information is being generated exponentially faster than at any other time in history. Privacy has basically gone out the window, and it's no wonder that headlines about data breaches have become commonplace.

In the past fifteen years, the Internet has revolutionized the way business is transacted, the way we communicate with each other, and the way we learn and research. E-commerce transactions and online banking and investments occur every micro-second, and sensitive information is exchanged for each of those activities. People sign up for free e-mail accounts and chat. Social networking sites invite us to post information about ourselves and we do so, often without even a thought as to what we are telling the world about ourselves. We go to school online. "Wiki's" and research sites have replaced hardcover encyclopedias in many cases. Many of us choose the Internet to obtain news, sports, and weather rather than newspapers.

Over this amazing period of time, it has become more convenient to keep information than to get rid of it. This brings up an interesting change in risk exposure when it comes to records retention for organizations such as schools and businesses. Are we retaining too much information and is it exposing us to data breaches or legal problems?

# To Retain or Not to Retain? (cont.)

By Kevin Doyle, CISSP, ISSMP,  
CISM

Advances in technology have allowed us to accumulate more and more information. Can you imagine how much paper would be needed if we converted all of our electronic data into paper files? Would we retain as much information if it was not for the technology age?

It has become more convenient for organizations to “retain everything” than to have a sound document retention plan and policy, based on legal requirements, risk, and common sense. We accumulate all of this data, and we store it on electronic media and ship it off site. Are we keeping track of all of the data stored on site and off site? Are we classifying information into what should be protected, such as private information, sensitive trade secrets, etc? What about the risk of the document custodians losing some of that information? Another hazard is retaining too much information related to something that might become a legal issue, such as an employee termination. When the subpoena comes along, it orders all information and communications related to this employee. Got e-Discovery?

Is there is adequate tracking so we retrieve only the information that is needed? Is data being de-duplicated? Are we keeping several copies of the same information? What if media gets lost in transit? Should we be encrypting?

The risk landscape for retention of information has changed dramatically in this age of technology. Management, along with attorneys and regulators, have to decide what information should



# To Retain or Not to Retain? (cont.)

By Kevin Doyle, CISSP, ISSMP,  
CISM

be retained and for how long. The best records retention policy is not to retain information, unencrypted forever. A policy based on legal requirements and risk is the soundest approach to records and document retention.