Secure Document Management

By Mike Ahmadi, COO

Contents

Introduction

We live in an age where documents are transitioning from paper-based to electronic formats. This has created an environment where documents can be archived, indexed, tracked, and managed in seemingly endless ways. Companies which once specialized in systems that printed, copied, and otherwise managed documents have wisely begun to make the transition into document management service providers.

In making this transition, a paradigm shift in the way documents are handled has emerged. Questions have arisen, such as:

- What format are documents stored in?
- Where are documents stored?
- How do we access the stored documents?
- What is the cost benefit associated with electronic documents?
- What are the security risks?

While providers of document management systems are well versed in addressing many of these questions in a highly qualified manner, the question of security is one area where challenges are often met with assumptions, and no real understanding of the objectives of a secure document management system.

The Problem

Security is a very confusing concept to most people. We know it is important to have security. We also know that not having security causes problems that are both obvious and not so obvious. When addressing security needs of an organization, as it relates to document management, you are often forced to make some assumptions, both consciously and subconsciously. These assumptions can sometimes be taken for

granted and may include some of the following:

- User access to sensitive information is to be limited by organizational policy.
- A security mechanism of some sort exists to prevent unauthorized access to documents.
- An auditing procedure has been established to track the access of and chain of custody of documents.
- A "doomsday" procedure is in place to mitigate risk of security breaches.

This is certainly nothing new, as such management practices have been in place within organizations for literally hundreds (if not thousands) of years. Previous generations have created systems to deal with document management that have become well established, clearly defined, and understood.

Modern electronic document management systems, however, have completely changed the way management must manage these systems. In creating a system which creates ease of use, a system has also been created which forces us to reevaluate security risks. Document management system providers are indeed aware of the need for security, but the traditional approach has largely centered on a very low-level solution. Emphasis is placed on software and hardware based security features, without going into a high-level analysis of system as it relates to business process. This unfortunately does not create a secure environment. All it creates is the perception of security. For some, perception is all the reality they may have a need for. It may be enough to address the compliance and liability issues they may potentially face, as the organization may feel that the implementation of any type of security measure whatsoever may be enough to serve as evidence of due diligence. For others, having the appearance of security is simply not enough. They need to be secure in order to prevent the loss of huge sums of money, or corporate secrets, or even human lives. How can a document management company properly address the needs of such customers?

Previous Options

As annoying as management of paper documents was in the past, and continues to be today, security was fairly straightforward. Let's address some of my previous bullet points:

- *User access to sensitive information is to be limited by organizational policy.*

  This is fairly easy to deal with. If the receptionist wants to look at corporate documents, you tell her no. If she decides to walk across the office into the document storage area, you stop her and ask her what she is up to. The threat always exists that she could misrepresent herself (perhaps she is a master of disguise), but, in all likelihood, you are going to be able to stop her before she gets

too far. If she does make it into the document room, however, there is always the next step…

- *A security mechanism of some sort exists to prevent unauthorized access to documents.*

  Hopefully, sensitive documents are in a locked filing cabinet. Very sensitive documents may be stored in a fireproof vault or safe. Breaches to these systems require time, exposure, physical access, and a lot of nerve. Once again, unless everyone in the office is sound asleep, it is not likely that this will be a problem.

- *An auditing procedure has been established to track the access of and chain of custody of documents.*

  Sensitive documents are often viewable only in a physically secure environment, without access to a copying machine or other duplication device. Protocols have been established to track documents from check out to check in. Physical access and accountability is often mandated in such cases, and management of documents in this manner is straightforward.

- *A "doomsday" procedure is in place to mitigate risk of security breaches.*

  If any level of security is breached in an environment with paper documents, it is fairly easy to recognize, and steps can be immediately taken to prevent further intrusion. Security staff can be summoned to secure exits, conduct searches, or summon law enforcement. Damage control measures are often quite effective in these scenarios, and scalability of intrusion is generally minimal or non-existent.

Given the expectation levels for security that have naturally evolved out of these and many other examples, how can a document management company insure an equivalent level of security when dealing with electronic documents? Does the organization that implements an electronic system for managing documents face any potential liability for not addressing these issues? When competing for business, does the system provider who recognizes that these issues exist and addresses them with the customer gain an advantage over the competition, especially since the competition faces these very same issues?

GraniteKey Solution

GraniteKey takes a very holistic approach to security. Through the use of our Attack Taxonomy, we determine the threat model associated with a system implementation, and provide and in-depth analysis of involved risks. We feel it is vital for the customer to clearly understand security risks, and make informed decisions based on

a high-level understanding. GraniteKey can provide training to sales and management staff within your organization to help you not only close more sales, but also protect your organization from potential legal issues.

GraniteKey also works closely with manufacturers who can build secure cryptographic hardware modules for implementation within a system, should the need arise. Again, we are agnostic to the technology, as we feel it evolves naturally as a result of the high-level assessment.

Benefit 1: Informed Staff

By understanding some basics of applying a threat model and risk analysis to a secure implementation, your staff can make better and more informed decisions with respect to your customer needs.

Benefit 2: Decreased Liabilities

When all parties involved clearly understand all the risks associated with a document management system your organization greatly mitigates its legal risks due to disclosure. When addressing security questions, you can then intelligently answer them by framing them with circumstantial qualifiers. In other words, it is secure "under these circumstances". While your competition may choose to dance around this topic, you can address it directly, and point out that your competition is not addressing this. Besides decreasing liabilities, this gives your customers more confidence in not only your ability to meet their security objectives, but in their own abilities as well.

Benefit 3: Increased Sales

Let's face it; you are not a printer, copier, Fax Company. You are a service company. Every opportunity you are given to fulfill a customer's needs is an opportunity to lock him in. If you can show your customer that you take the security of their documents more seriously than your competitors, and security is indeed your customer's need, then you score a win.

Implementation

GraniteKey can, first and foremost, train your staff in understanding how to take a holistic view about security. We discuss high-level concerns in great detail (business process, threat models, risk management, etc.), and also go into detail about low-level security technologies (cryptography, encryption, key management, etc.).

In circumstances where real security is paramount (government, military, financial systems) we can work directly with your customers to define the security target and propose real solutions based on our analysis of the environment. In circumstances where the customer wants security for the purpose of compliance (quite common), we can help you assess the environment for the purpose of mitigating your liabilities.

Summary

Building confidence between your organization and your current and potential

customers is beneficial to both you and your customers. When you enlighten your customers you become a valuable part of their organization through the trust bonds you develop. By offering solutions which show you are thinking "outside of the box" you not only capture their attention; you capture their checkbook as well!

268 Bush Street
#3350
San Francisco, CA 94104-3503
http://www.GraniteKey.com
P: (925) 413-4365