

Best Practices – Improving Document Security

Understanding how to keep your company secure can be a moving target. From cyber-criminals hacking high-profile websites to complex identity theft scams, the media seems to report a new attack almost every day.

Unfortunately, recent statistics substantiate this thought. Javelin Strategies, a prominent research firm, reports that incidences of identity theft increased by 11% from 2008 to 2009, and affected the lives of 11 million Americans. Considering that this crime has been on rise for multiple years, if these numbers prove to be a pattern, one in every 20 Americans risks being a victim in 2011. That's a scary thought.

With these statistics in mind, it is important that individuals and businesses take steps to protect their information – and themselves – from such an incident. While high-tech crimes garner much of the media attention, low-tech crimes such as stealing someone's wallet, checkbook or trash cause almost half of all crimes.

It follows that understanding and implementing secure document handling procedures must be a priority. Many business owners are asking, *"What constitutes document security best practices?"*

1. **Examine the entire document lifecycle.** Before you can identify any security vulnerabilities, you must first understand your company's document workflow and lifecycle. From creating the documents to storing and transferring them, many documents touch multiple departments and personnel. The more touch-points, the greater the risks.
2. **Develop security policies.** By creating an internal document handling process, employees will have a clear understanding of what constitutes a sensitive document, how to handle them properly and what to do in the event of a potential breach or suspicious behavior. Additionally, it is important to research national and local legislation to ensure your new policy is 100% compliant with rules and regulations.
3. **Limit access.** The more people who have access to sensitive documents, the greater the risk of a theft or breach. Restrict employee access to confidential data. This should be done based on specific business needs or specific categories of personnel. From limiting access to the record-keeping room to locking filing cabinets, there are many ways to accomplish this task.
4. **Perform training.** Ongoing updates to privacy legislation and personnel changes mean that it's not enough to simply create a privacy policy – it also must be adapted and reinforced from the top down. It makes sense to implement quarterly training or retraining sessions so the privacy policy is easily understood and followed.
5. **Destroy documents securely.** Confidential documents must be destroyed once they are no longer needed or the legal retention period is met. Secure destruction means they are shredded in such a way that the document cannot be reconstructed, and the intact document is not exposed to risk prior to shredding. This can be accomplished with a regularly-scheduled on site shredding service.
6. **Build a culture of respect.** With all of the potential hazards for security breaches and identity theft, a company can only minimize the risks it faces, as opposed to eliminating them entirely. Therefore, the company needs to create a culture that values and respects confidentiality and privacy. Employees will be better educated and motivated to adhere to the privacy policy and treat document security as an important company initiative.

With so many moving parts, it is clear that building a comprehensive document security policy requires commitment, resources and an internal champion. In order to help you begin, it may make sense to consult an expert in document handling best practices or secure shredding solutions. Once you've developed a plan and an implementation strategy, you'll have taken an important step in protecting your company and customers' privacy.

