SECURING THE FUTURE

Shred-it

Secure Document Management & Destruction as part of Crisis Planning

We all recall seeing the video footage of hurricanes and violent storms blowing through cities with a whirlwind of paper always in view on the TV screen. That paper, possibly financial data, medical records or personnel files, could have been shredded as part of an ongoing crisis plan to prevent its distribution to potential thieves.

"We know that when sensitive documents, such as legal files or medical records, are unsecured, they are at risk of being misplaced, misused or stolen, which can lead to long-term financial, legal and reputational issues. But consider the equally hazardous risks that they can also be carried away during a severe storm, scattered outside during a fire or simply become more vulnerable in the disorder of a blackout," says Mr. De Palma. Even if documents are already partially destroyed, they may still be targets for identity theft. For instance, wet paper may look useless, but a thief with a blow dryer could use it to steal information about your business, your associates or clients.

Document management and destruction should not be left to chance or discretion of individual managers or employees. There must be a strategic, systematic, companywide effort that addresses information security at all levels. While there is no single recipe for success, information security measures that are applicable to most organizations include:

- Restricted or differentiated levels of access to sensitive electronic records.
- Secure storage of paper documents in locked cabinets.
- Disposing of office paper waste in special security consoles.
- Regular onsite document destruction, using cross-cut methodology that transforms paper documents into unidentifiably small pieces.
- Consistent information security policies, whose implementation is supported by the commitment of the senior team and an overall security culture.

Implementing these measures means, there are no unattended files sitting in the corners of your office – they are either filed away securely or completely destroyed. This means that, should an emergency strike, the risk of an information security breach is dramatically reduced, regardless of what happens with the rest of your company's waste. Destroyed information is no longer a threat, and paper waste securely locked in consoles is harder to access even if submerged in water, fire or snow.

Modern organizations are susceptible to all sorts of disruptive events. Among them are fires, natural disasters, power blackouts, terrorist attacks, national pandemics, cyber attacks and information security breaches. In this age of increased security threats, the growth and survival of your business depends on its ability to function and manage, even through a crisis.

Over the last 10 years, we have witnessed 9/11, the Northeast Blackout of 2003, SARS and the H1N1 influenza outbreak and watched Hurricanes Katrina and Ike crash into major cities. What else is coming down the road?

While the likelihood of a serious emergency may appear low, the recovery costs from even a low-scale disaster are often high. Simply put, your business cannot afford the risk of being unprepared for disruptions. That is why it is important to have comprehensive plans in place that address a wide range of emergency scenarios. While crisis responses are multi-faceted, they should always include an information security planning component. An information security component can avert a potential information breach and with it the associated financial loss and reputational damage.

"At Shred-it, we believe that prevention is the best crisis planning tool," says Vincent R. De Palma, President and CEO at Shred-it. "To avoid a disaster-related information breach, all information, in both paper and electronic form, must be secured, regardless of where it is located. Likewise, all information that is no longer needed should be destroyed."

Two added challenges are that prevention and information security preparedness are very difficult to coordinate in the short-term before a forecasted disaster strikes and near impossible to coordinate with an unforeseen disaster. Yet, with some forethought, these scenarios are relatively easy to avoid.

In this Issue

Small businesses especially at risk

The private sector, which comprises an enormous portion of the U.S. economy, is an important player in the protection of our safety and security. Yet, smaller organizations tend to have a more lax security environment.

- SMBs may not have formal information security policies and procedures in place. Many SMBs cannot afford the financial blow of a security breach, with the average cost of fraud to organizations of all sizes reaching $8.8million in 20091.
- SMBs may have limited access to legal resources, with no internal legal team available for support.
- SMBs often have no HR departments that can consolidate and protect employee records.
- They often have no restrictions on internal information access by their employees, including temporary contractors.
- During the hiring process, they typically do not require extensive security checks on their future employees.

One of Shred-it's small business clients2 recalled that, when taking over a small accounting firm, he was surprised to discover that all paper waste used to go to regular garbage boxes and had been left unshredded outside of the building for pick-up by municipal garbage-collection services.

Information security recommendations from Shred-it

There are two important tenets behind all best practices in secure document management:

✓ All sensitive information that is no longer required should be destroyed.
All sensitive information that is not destroyed should be stored securely.

Shred-it advocates a tight chain of custody around the entire document management process that should be implemented in a strategic, systematic way. Below is a list of best practices that forward-looking organizations follow to protect themselves, their clients, employees and other stakeholders during normal operations and in an event of emergency:

01 **List all information security risks:** specific to your organization, targeting both paper-based and electronic information sources; consider every stage of the information cycle, from data generation and storage to the transfer of data from location to location and the document destruction process.

02 **Develop data security strategies:** that address each of these risks.

03 **Commit to total information security:** have a clear vision of why your organization is implementing these measures and have the systems in place to make it happen – clear policies, and appropriate communication, training, and management processes.

04 **Train your staff** in document destruction policies and best practices; offer training courses, which may include general security training or specifically deal with secure document destruction; best practices can be summed up as four principles that are easy to understand:

- **Shred all** – to avoid the risks of human error or poor judgment.
- **Shred regularly** – to deter the accumulation of confidential paper waste.
- **Shred securely** – to ensure the chain of custody meets your compliance requirements.
- **Shred before recycling** – to avoid risks once confidential paper waste is at the recycler.

1 http://www.kroll.com/about/library/fraud/Oct2009/downturn_and_fraud.aspx
2 Tom Corley, president, Cerefice & Company in Rahway, New Jersey

Sign up for your free security consultation

As security and public safety threats are more intense than ever, the need for secure business continuity planning is clearer than ever.

To learn more about Shred-it services or to book your FREE security audit, visit http://www.shredit.com

Shred-it is a world leading information security company providing services that ensure the security and integrity of our customers' private information. The company operates 140 services locations in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies and more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.

To learn more about Shred-it document destruction service, contact us at:**1 800 69-Shred (74733).**