

SECURITY CHECKS AND BALANCES FOR GOVERNMENT

Best practices in secure document destruction from Shred-it

Technological innovation is changing the information environment and operational practices of many organizations, and government – including its national, municipal and provincial levels – is no exception. Government databanks, starting to integrate pools of biometric data, are increasingly digitized. At the same time, the documents in traditional paper form are still a regular fixture of the government departments, agencies, boards and commissions. Given the magnitude of the data stored within government organizations and the consequences of potential security violations, it is important to understand security risks, learn from best practices and implement the measures needed to achieve total security of government information.

This case study will discuss common challenges and best practices in secure document destruction, identified by Shred-it, a world-leading information security company, in the course of its 20-plus years of experience working with government clients around the world.

DEVELOPING A HIGH-SECURITY DOCUMENT DISPOSAL PROCESS

Most government organizations have a process in place to deal with their paper waste, typically incorporating shredding and recycling components. The process is managed either in-house or by a third-party provider. However, the level of security of different document destruction methodologies varies dramatically, based on how they address the following questions:

- Is all paper waste fully destroyed on a regular basis?
- How and where are paper documents stored before they are destroyed? Are there any security loopholes along the way?
- Is the same document management and destruction process consistently implemented throughout the organization?
- Are all staff committed to the integrity of the document destruction process?
- Are there formal policies in place governing the issues of information security, such as employee access to sensitive information?
- Is there formal training in secure document management and disposal? Are all employees fully trained?
- What are the overall attitudes and culture around managing the paper trail?

“Each of these questions sheds light on whether a particular government organization has a comprehensive document security strategy,” says Doug Dawson, Major Accounts Executive

and government sector expert at Shred-it. "In fact, we recommend including them in government security audits that should be conducted periodically or, even better, on an ongoing basis."

ADDRESSING POTENTIAL SECURITY LOOPHOLES

Certain practices that organizations use to store and dispose of their confidential data create the potential for this data to be mishandled. Dawson, who oversees a number of government client relationships, notes the following common security risks in the government context:

- Disposing of documents in ordinary garbage or blue recycling bins.
- Negligence or wrongdoing of government employees, who may abandon, leave unsupervised, lose or, in certain cases, steal or share confidential data with unauthorized outside parties. This type of breach can occur in paper form or on laptops or portable storage devices.
- Lack of formal policies and secure document destruction procedures due to budgetary concerns.
- Lack of training for government staff on information security policies and procedures; lack of adequate employee understanding of what government information should be protected and securely destroyed.

In the government context, employee education in secure document management and destruction cannot be overestimated. Maintaining comprehensive policies that address all kinds of information security scenarios is imperative, but it is not enough. All US federal agencies, for example, have formal policies and procedures in place governing information security at various levels, including non-classified, classified and top-secret information. All employees are expected to know these requirements, with some very specific directives for specific security situations. However, no matter how comprehensive, these policies will only achieve their purpose if employees know them, understand them, commit to them and follow them.

"If some employees continue to take home laptops or briefcases with sensitive information, that raises a question whether policies are truly working," says Dawson. "More often than not, this is a matter of education. For example, there may be formal training required for all new employees, but if refresher training is overlooked or put off to accommodate other priorities, employee awareness and commitment with regard to information security may start to wane."

What government employees do with the documents they no longer need is another major area of concern. For example, instead of sorting classified and non-classified information and following proper document disposal procedures, some employees may be tempted to discard all paper waste into recycling bins or put documents in a bag and burn them. Such situations may also be a result of insufficient knowledge and understanding, which, ideally,

should be reinforced through recurrent training in secure information destruction policies and procedures.

As for what these policies and procedures should be, most forward-looking government organizations realize sooner rather than later that simply throwing their confidential documents in the recycling bin is not secure. Shredding them in-house, when large piles of paper accumulate in unprotected areas, does not provide a sufficient level of security either.

There are also economic and compliance considerations at play. "In-house shredding is expensive because it consumes valuable employee time," says Tom Hunter, Account Manager, Shred-it. "And, when it comes to compliance, government is judged by a higher standard than any other organization." Most countries have legislation to protect the privacy of their citizens' information. Typically, such legislation places the onus of protecting sensitive information on the organization collecting it. The costs of non-compliance – financial, legal and reputational – may be very high, both for the organization in question and for the individuals affected, far outweighing the costs of implementing secure information management and destruction processes. In the case of government, there may also be additional national security implications, with their respective costs. However, important as they are, cost and budget considerations should never override the government's overall commitment to the integrity and security of the government information at all levels.

INTEGRATING DOCUMENT DESTRUCTION BEST PRACTICES

The policies increasingly embraced by government organizations around the world are "shred-all," "shred regularly," "shred on site" and "shred before recycling." Working together, these policies ensure a tight chain of custody around the entire document destruction process and essentially eliminate human error. At the end of each and every day, all waste paper goes directly into locked security consoles specifically designated for shredding. All paper documents stay there until destroyed at regular intervals by professional staff. Only after destruction, when transformed into unidentifiably small pieces, are the document pieces ready to be recycled.

These policies tend to take root in government organizations where document security best practices are embedded both in employee mindsets and in operational processes. Here are some of the measures such leading organizations typically pursue:

- List all unique information security risks specific to their organization, targeting both paper-based and electronic information sources; analyze every stage of the information cycle, from data generation and storage to the transfer of data from location to location and document destruction.
- Ensure full compliance with government security clearances and standards, as well as national privacy and identity theft legislation.
- Train government decision-makers in best practices in secure document management and destruction.

- Implement environmentally sustainable document destruction practices, where document destruction is followed by recycling of the shredded material.
- Outsource document destruction to high-quality professional providers, whose methodology ensures the total security of the document disposal process. Look for a professional provider that offers:
 - Powerful shredding machines that can quickly destroy large volumes of paper, using cross-cut shredding rather than strip shredding technology.
 - A policy that allows customers to view the full document destruction process.
 - Certification documents which confirm paper waste has been securely destroyed after every session.
 - Special on-site security equipment for customers such as locked security consoles.
 - A tight chain of custody that bypasses any storage, shipping and other steps which create potential security loopholes.
 - A standardized document destruction service that is offered nationally or even internationally.

In Canada, Correctional Services of Canada is among the leaders in the adoption of secure document destruction practices. "We have records management and security policies demanding that we handle information in a particular manner, including how it is stored and shredded. Much of the information we deal with is personal information, therefore it must be cross-cut shred, rather than destroyed utilizing personal strip shredders," says Claudette Jefferson, Regional Chief Administration, Correctional Services of Canada.

"Previously, documentation destined for shredding would be stored by individual offices, and then forwarded to my attention to arrange for shredding. This practice was not efficient as storage space was at a premium, and it left us vulnerable in terms of safeguarding information."

Edouard Larocque, Manager, Accommodations and Acquisitions, Health Canada Bureau of Strategic Initiatives and Planning, shares his experience: "Everything was going to a recycling bin before. Having conducted an internal audit, we were not entirely comfortable with everything being recycled and wanted to close the loop. When office waste is recycled, without prior shredding, you don't know where it goes. It could go to another city, for example." Now, all seven bureaus in Larocque's marketed health products directorate uses Shred-it. "We have a much better comfort level, and I can sleep at night," says Larocque.

The UK's Civil Service went through a similar process of re-assessing their information security systems. The UK's Home Office Pay and Pensions Service (HOPPS) processes the wages for 85,000 employees each month and administers the Civil Service Pension Scheme for 81,000 members, generating a large amount of confidential waste. Before signing a contract with Shred-it, HOPPS, whose paper waste used to be destroyed by another

provider off-site, did not have the peace of mind that the data had been disposed of securely. That is why its management decided to work with a vendor providing on-site document destruction.

THE SHRED-IT SOLUTION

Working with hundreds of government organizations worldwide, Shred-it, the world's leading information security company, is well-versed in the unique document management and information security challenges of government. It knows that government clients expect much more than just destroying documents. They need a strategic partner that delivers best-practice solutions, while also consulting and educating government decision-makers on how to identify and proactively manage their information security risks and how to make their operations environmentally sustainable and cost-efficient.

Larocque comments on the reasons why his organization chose to work with Shred-it: "The level of shredding they offer meets our needs, and is quick and easy. The service is on-site, we're able to watch it and get the Certificate of Destruction right away, and there is a much tighter chain of custody. Documents that go missing here could easily end up on the front page of the newspaper, and that's not good for anyone. Currently, Shred-it's services are used by the treasure board, security department and by the entire branch."

Philip Elliott, Home Office Pay and Pensions Service in the United Kingdom, also stresses the security aspect of the on-site document destruction methodology offered by Shred-it, which currently services their department on a weekly basis. "Shred-it provides references from other government agencies, which gave us peace of mind that other offices with sensitive material were happy with Shred-it's services," says Elliott. "More importantly, Shred-it destroys the confidential data on-site. We could witness the data being destroyed and receive a Certificate of Destruction after each visit, providing us with an audit trail for our confidential material."

In the United States, Shred-it has been awarded a Government Services Administration (GSA) pricing schedule, allowing access to approved vendor status that governments require to employ vendor services. The U.S. General Services Administration is a central management agency that sets policy price schedules for federal, state and local governments. Being on its pricing schedule allows agencies on all levels to take advantage of the secure document destruction services provided by Shred-it.

Environmental sustainability is an important consideration, too. The recycling component of secure document destruction, offered by Shred-it, allows government organizations to minimize their negative environmental impact in a measurable way. "We have saved 75 trees since we started working with Shred-it," says Larocque. "Being green is a concern for us. We have a whole green procurement strategy, so this just helps towards that and supports our environmental goals."

In summary, here's how Shred-it addresses the needs and concerns of its government clients:

- Work alongside government managers to come up with customized solutions to protect sensitive information.
- Adapt to the budgetary restraints affecting government institutions and develop document destruction solutions that are both high-value and cost-effective.
- Provide the highest level of security in the document destruction process.
- Facilitate government employee and management training in secure document destruction processes.
- Employ best practices developed over the company's more than 20 years of document destruction experience.
- Assign pre-screened, bonded and insured customer service representatives.
- Provide a "Certificate of Destruction" upon completion of the document destruction process.
- Invite the government staff to view the document destruction process.

Secure document destruction is one of the checks and balances that ensures the security of government information. It also saves costs, increases employee productivity and enhances the reputation of government organizations. Investing in secure document destruction is a far better investment than paying the costs of security breaches, which may lead to serious psychological, legal, reputational and, potentially, national security implications.

About Shred-it

Securit | 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 branches in 16 countries worldwide and has more than 20 years of experience 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. Securit | Shred-it offers three primary service lines: Records Management, Data Protection, and Shred-it Document Destruction. For more information, please visit www.securit.com and www.shredit.com.

Shred-it contact information:

1.800.69 SHRED

shredit.com



Making sure it's secure.