A SIMPLE GUIDE TO SECURE DESTRUCTION

Mona Lai
Group Head of Business Development
Crown Records Management

The power of memory

crownrms.com

CROWN
RECORDS MANAGEMENT

CONTENTS

CHAPTER 1

WHY SECURE DESTRUCTION IS RISING UP THE BUSINESS AGENDA

There's no better time to be thinking about secure destruction than right now given the increased risks that businesses face in the modern world, the greater reliance they have on data, and the market pressure to modernize information management systems.

Let's be clear, secure destruction is not a new service - it has been around a long time but has taken on new relevance thanks to trends emerging from the pandemic, new data protection regulation and the increased volume of data and documents being stored by businesses of all sizes.

Now, in the wake of the pandemic, the need to embrace secure destruction strategies is greater than ever.

The need to save money

At a time when some businesses are fighting against the tide, the need to make savings is obvious. So why are so many continuing to store boxes full of documents which no longer need to be kept? Significant savings can be made in long term by destroying documents which are past their retention date.

The impact of the working from home boom

Not only we are collecting more data than before but the adaptation of hybrid working, with many employees working from home, the risks involved has dramatically increased.

A business can have all the correct procedures and protocols in place in its offices and warehouses, but how can you control what's happening in the homes of your employees?

Systems have been put in place at many companies allowing employees to access data and workflows; and with that comes extra risk.

It is possible and advisable to introduce restrictions on printing from home to help prevent unnecessary duplicates.

However, the risks for electronic data are rising, too. Having duplicate data which is stored outside of the system can lead to data breaches or to a failure to delete or destroy data which is past its retention date.

This can lead to laws being broken and increase the likelihood of data falling into the wrong hands including rival businesses. Secure destruction is the answer.

The rise of data protection regulation

In addition, the rise of data protection regulation across the world means companies are at risk of significant fines if they suffer a data breach or fail to look after the personal data of customers and employees.

A good example is GDPR in Europe, but this kind of regulation imposes obligations onto organizations anywhere and is also mirrored in many areas of the world.

There are many data privacy and information security regulation, please check APRA CPS 234, PCI DSS.

The risk on paper

Despite the digital revolution, paper remains one of the core reasons for a secure destruction policy.

Many years ago, we were told that the rise of electronic data would lead to the paperless office, but we certainly aren't there yet.

There are still many people who instinctively print hard copies of data and are more comfortable working when they have a piece of paper in front of them. If they bring the habbit to home, that will even raise more concerns.

Some sectors, such as law and banking for instance, are still heavily wedded to paper in many regions of the world and are just changing their ways during a time when offices were closed because of the pandemic.

Paper records can also be a risk in the office environment, especially when companies do not have a procedures for confidential waste destruction and throwing paper away along with other general waste.

It might seem like a low-risk and low-cost option but in fact there are criminals out there willing to look through bins and search for sensitive data – whether stored in offices or at the personal homes of employees. It's not a widespread crime but it does happen, and it is certainly an uncomfortable experience for businesses when it does.

The criminal risk

A rise in cybercrime is another significant driver for secure destruction.

Cyber criminals prey on companies which fail to look after data, ready to steal personal data for profit. This may be even easier to do when employees are working from home, especially if they use a personal computer. Every piece of data that is kept unnecessarily instead of being destroyed adds to the risk.

The need for secure destruction is clear, so here is our simple guide on how it can help a business and how to start the journey…

A SIMPLE GUIDE TO SECURE DESTRUCTION: THE KEY QUESTIONS AND ANSWERS

By Kevin Moore
Crown Records Management,
New Zealand

What is secure destruction and what can I destroy?

Secure destruction is primarily the permanent destruction of data – both physical and electronic, hardware, and other products which would provide risk to a business if kept unnecessarily.

Almost anything can be destroyed by professionals, but the most common example is records and data which are stored on paper, either inside a business or in the warehouse of an outsourced company.

As technology moves on, however, increasingly we are also looking at electronic data saved on servers or hard drives – anything from emails and social media messages to spreadsheets, customer data, employee HR data, company accounts, supplier data, or minutes of meetings.

It may also include computers, printers, and other hardware on which data is stored. These days, with the Internet of Things (IoT) gaining popularity, there are many products which 'talk' to each other and store data – from photo copiers to speakers and even fridges.

One client, a high-end manufacturer of goods for high-net-worth individuals, wanted unsold products destroyed rather than create the appearance that they were unpopular.

Why should I consider secure destruction?

It's best to think of secure destruction as a form of insurance.

If you have data which you value, or data which would be a risk if it ended up in the wrong hands, then secure destruction is a way of lowering that risk.

It might prevent a business from ending up with a big fine for a data breach or ensure that rival businesses don't gain a competitive advantage by gaining access to data you don't want them to see.

> **Think of it this way. If you are a good driver, you still need insurance and most people accept it is necessary.**

What if my business already looks after data well, do I still need secure destruction?

A secure destruction policy means you remove all outdated data from the business which doesn't need to be there.

Some types of data MUST be deleted by law after a certain period. In New Zealand, for instance, it is illegal to keep employee data for more than two years after they have left the organisation.

So, how long should I keep data for?

This depends on the type of data, the industry, and the region a company is based in.

Governments often set rules on how long data should be kept for and when it should be destroyed.

How do I know if it my data has been securely destroyed?

A certificate can be provided which confirms the secure destruction of data.

It is also often possible to watch the process; top secure destruction companies will have security cameras, for instance, and most will be happy for an IT manager or business manager to be there in person.

Is there a global standard for secure destruction?

There are national standards in many different countries but not a single global standard.

The standards set by the North American Association of Information Destruction are accepted by many businesses across the world, but there will always be clients who want to go a step further. It's about choosing how you want the data to be destroyed and how impossible you want to make it for someone to retrieve the information.

How do I work out if secure destruction is good value?

There is a cost to secure destruction, but the benefits come from peace of mind, compliance, and the mitigation of risk.

In financial terms, the difference between the cost of a general waste stream and secure destruction is the real figure to consider.

But how much value do you place on the threat of sensitive data falling into the hands of a rival business? Or on the threat of a data breach or a data protection fine? Or a loss of reputation?

These are complicated aspects to evaluate with a figure because every business is different.

What is best depends on what a company needs destroyed and the risk level of the data.

What types of secure destruction are there and which is best?

Consequently, to what lengths it is willing to go to ensure it is impossible to ever recover.

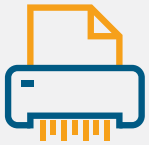
Many businesses choose to combine two or three of methods when they are destroying highly sensitive data – and they will often ask to come and watch it being destroyed.

The most common type of secure destruction is shredding, but we're not talking about the kind of home shredder which is sold in the High Street and shreds paper into strips.

There have been horror stories of criminals stealing bags of this kind of shredded waste put out by the cleaners at major companies - and then painstakingly putting them back together to gain information which gives them a competitive advantage in the marketplace.

Advanced shredders used by secure destruction experts can shred just about anything, from paper to credit cards, CDs to DVDs, and even hard drives.

The many ways of destroying hard drives:



Shredding – popular for paper but also regularly used for many other items depending on the machine, including hard drives.

Incineration – this method comes with environmental issues but remains popular in some areas of the word. It requires two chambers, each with an internal temperature of 1000 degrees Celsius.

Degaussing – data is wiped from media using a strong magnet.

Hydro Pulping – in addition or instead of shredding, this involves the paper being pulped and the ink removed so that it can be recycled.

Crushing – a way of destroying hard drives, phones and laptops using a crusher with a steel punch.

Grinding – a machine which grinds items to dust, ensuring any data on them is unrecoverable. Some machines grind down to 2mm particular.

What other benefits does secure destruction bring?

The reputation of a business and its ability to attract and retain talent is partly determined by how well it looks after data – and in countries where that isn't the case yet, it is still the direction of travel.

Privacy and data protection are now high-profile topics and high in the public perception, too.

People care far more about their personal data than ever before and for the first time, they understand its value.

What are the sustainability credentials of secure destruction?

There are different aspects to the ways that secure destruction can fit into the circular economy.

When securely destroying physical data on paper, pulping ensures the end product does not go to landfill and can be re-used.

This is an increasingly important secondary benefit for businesses who are chasing Net Zero targets, and secure destruction companies will be able to provide figures on how much of the product was recovered and how many carbon credits that might amount to. Certainly, when it comes to paper-based secure destruction, you are talking about recoveries in the mid to high 90 per cent region.

It is important to separate paper and non-paper in secure destruction bins to help this process, another education piece for employees.

How does secure destruction make life simpler?

We've talked already about secure destruction being like an insurance policy and it's one that helps directors feel more confident that their company's data is not going to cause problems.

By putting strict retention policies in place and then supplementing them with a secure destruction schedule, the process can help remove stress in the boardroom.

The threat of big fines for data breaches, of legal cases for breaking the law or of rivals getting their hands on sensitive market information are greatly reduced.

By using an external secure destruction expert to look after the process, dealing with collection, destruction and certification, business life is made simpler.


CROWN
RECORDS MANAGEMENT

CHAPTER 2

AROUND THE WORLD OF SECURE DESTRUCTION

Advice, insight, and top tips from Crown Records Management experts across the globe

The ways in which documents and data are securely destroyed, and the benefits of doing so, are similar the world over. But that doesn't mean that all regions look at secure destruction in the same way or have the same drivers.

Here we talk to Crown Records Management experts from across the globe for their insight about the client experience in their region and why secure destruction is rising up the corporate agenda.

Peter Burton
RMS Division Manager, Philippines

What is the biggest issue in secure destruction for clients in your region?

In this region, the vast majority of data we handle is still physical documents in boxes and this is driven by the regulatory process in certain business sectors, especially banking and finance, where businesses are required by law to keep documents for a long time.

There is a lot of red tape and bureaucracy across the region and businesses are only able to destroy some physical documents once they have been kept for 10 years. So that's a huge number of boxes and physical files being stored.

Even so, there are very few companies offering secure destruction across Southeast Asia, perhaps just three or four globally recognized names, because clients are nervous about breaking rules and don't trust smaller local providers.

Part of the value of Crown's offer is in understanding the policies in the first place. Many are quite ambiguous and differ wildly across Southeast Asia and particularly here in the Philippines.

What part has the pandemic played in moving secure destruction up the business agenda?

The shift towards individuals working from home and to more flexible systems, utilizing online data, has certainly had an impact. It's led to a change in strategy for many businesses. At Crown we've had increased demand for scanning and digitization of records, for instance.

But I have to be honest and say I don't see it as a long-term shift, unlike in other parts of the world. The move to flexible working is a slow burn and a lot of people are already back in the office here.

What is the situation with data protection regulation locally? Are any countries following the European model?

It's very early in the story, here. There's awareness of GDPR and other equivalents around the world, for instance in the US, but the focus is not the same.

In the Philippines, there has actually been a data protection law in place since 2012, the New Data Privacy Law. But most people don't understand how to comply with it or realize the penalties they can face by not complying.

There seems to be a conundrum here. New data protection regulation means you can be at risk – but many businesses are scared to destroy data because of complicated retention requirements.

That's exactly it. A lot of clients only come to us at the end of the cycle when the box has been kept 10 years and needs to be destroyed. What they really needed was someone to manage that data from the start, set a retention policy for it, and destroy it at the right time.

Can you think of an example of documents which people keep unnecessarily?

All records have different retention requirements and not all businesses are aware. For accounting and finance it's normally 10 years, for HR or personnel files it's seven years after they become inactive. Medical records are often subjected to rules requiring records to be kept for 25 years. Businesses need assistance in this area because many just 'play safe' and keep files indefinitely.

Not all data is physical. What about digital data?

In this area, clients are often wary of destroying data.

It's only now as businesses come to terms with data protection, mainly because of dealings with clients in the US and Europe, that they are starting to think about it. Suddenly the complexities are catching up with them and they want to know what to do.

"We're seeing a rise in requests to destroy digital data – anything from floppy disks and VHS all the way up to data stored on servers and hard drives."

If you look into future, do you think European style data protection regulation will get more prevalent in Southeast Asia and more relevant?

I do. Most of the laws which are being implemented across this region are based on GDPR but there is still confusion. There's not a lot of case study of what happens here if you violate the policy, so in terms of penalties and liabilities, it feels like a big unknown.

But, of course, no company wants to be the first to find out!

Rosena Rabbitte

National Commercial Manager, United Kingdom & Ireland

Has the pandemic changed the environment around secure destruction in the UK and Ireland?

I think it has. Businesses are looking more closely at what they're holding and the information they're keeping.

There are many reasons for this. First, a lot of people who were travelling before are spending more time behind a desk, either in their own homes or back in an office facility but unable to travel.

They've had more time to consider the issue and have a greater awareness of it. The pandemic accelerated a lot of decisions, too.

A customer asked CRM to move asked to move 6000 boxes in 14 hours to a location Outside of London.

Subsequently, the same company made a decision to bring forward their property strategy and closed a large number of offices – something they had previously intended to do over a longer period.

A lot of clients are thinking: we've got all this information stored, how much of it do we really need? Is there anything we can do to reduce our costs? What can we scan? What are the other options out there?

So, is a reduction in costs one of the prime considerations when thinking about secure destruction?

Absolutely, it's right up there. If you can reduce the number of boxes you store – and often it's possible to reduce the number dramatically – then you save money on storage and at the same time reduce risk. It's often the starting point for many clients.

As an example, one of our clients – an American bank – had 283,000 boxes with us and four years ago embarked on a big secure destruction project.

It was a complex operation because they had several separate departments which needed to approve and sign of the destruction of each document. But by the end of the process, the number of boxes stored had been reduced to 50,000. That's a big saving in ongoing costs for storage.

What puts people off secure destruction, then? Why hasn't every business done it already?

It's often a cultural thing. Many businesses have a strict culture around destroying documents and they are over-cautious. They keep documents 'just in case'. Even if they are past their retention date, and that's bad practice.

How often should documents be destroyed, then?

It depends on what they are. But it's a good idea to consider a planned secure destruction program which keeps everyone up to date. If you have items that are expiring every month, then it makes sense to destroy them as soon as their retention date is reached.

"For instance, one of our customers was worried about a London lockdown last year and feared they would be unable to access key documents as a result."

What impact is GDPR having on secure destruction?

It's having a big impact, because businesses are realizing that keeping information unnecessarily can be a risk when it comes to data protection.

But it's still early in the piece – a lot of companies are still acclimatizing to GDPR requirements. The problem is they don't even know what data they have, let alone what to destroy. So, that's where the journey often begins. First of all, find out what you've got!

In the past, information stored wasn't even classified or categorized, so it's often a big operation just to find out what you have in your boxes.

We were involved in an audit for a pharmaceutical client recently and we are usually asked to randomly select a number of boxes to look through. We opened one box and everything in there was in French – because they were from a clinical trial which had been transferred to the UK from France many years earlier. Nobody was aware what they said, without a translator, or why they were still being stored.

That's just a small example of how complex it can be to find out definitively what information your business is storing and whether it still needs to be retained.

Audits are another good reason to consider secure destruction, especially with GDPR. You need to have good reason to keep people's personal data now, and if you don't have a good reason then you need to destroy it.

What about destruction of digital data? Are the principles any different?

Not really – they are exactly the same. The method of destruction is different but the thought process and the reason for destroying is the same.

Of course, digital data is often governed by an IT policy and managed by the IT side of the business, so there may be parameters already in place. But the bottom line is that it needs a retention date, it needs to be securely destroyed at the right time – and it needs a certificate to show it has been done properly.

Pieter Nienaber
Office/Compliance Manager, South Africa

What's the situation and background in South Africa when it comes to secure destruction?

In South Africa we have a lot of physical documents that need to be destroyed. Many of our customers who have been with us for more than 10 years are waking up to that because of new privacy laws.

These were introduced in the POPI Act, which stands for the Protection of Personal Information Act.

It's very similar to the international data privacy laws in other parts world, such as GDPR in Europe, but there are also tweaks to make it more relevant to Africa.

For instance, you can be held responsible as an individual, not just as an organization. So, it's been defined to fit our own environment here in this region.

Fines for breaching the Act can be as high as 10m Rand – or even a jail sentence in extreme circumstances.

What does the Act focus on?

It's all about protecting personal data and protecting data subjects from harm if their information is not looked after properly – so for instance, from theft or discrimination.

One of the biggest focuses is on protecting account numbers and that has been well publicized in South Africa. So the most affected industries are financial services, healthcare and marketing.

There's also a big focus on retention dates. Records of personal information must not be kept any longer than is necessary for achieving the purpose for which the information was collected.

There are some exceptions, for instance when the data is required by law or contract. But it is no longer acceptable to keep personal data longer than is needed.

In terms of storage, personal identifiable information needs to be secured by a seal and can only be stored for three months here. Anything which is identifiable information, like log sheets or IDs, unless they are attached to any HR documents, need to be destroyed after that period.

As a result, a lot of clients are thinking much more about their retention policies when to review or destroy documents.

Has it changed the services which Crown Records Management offers?

We are offering destruction processes not only for clients who store boxes with us but for other companies, too. Businesses which don't work with us right now but want to destroy their documents. It's still a trackable service with a secure destruction process and a certificate of destruction at the end of it.

What other new services do you offer?

We are also offering bin rotations. We can hire out a secure destruction bin to customers, perhaps for a month or two weeks, and we then charge them per kilogram for the destruction of the company records collected in the bin.

It's a secure bin and once it is full, it is then transported by a trackable vehicle to our secure destruction center. A certificate is issued once the information has been securely destroyed.

We don't see many other records management companies offering this service and it's a popular one because of its simplicity.

The bottom line is that if businesses have documents which are no longer required but which contain business or private information, they need to be securely destroyed.

What happens to the paper once it has been destroyed?

This is one of the beauties of the service, because the paper is then pulped. This has two benefits. Firstly, it means any information which was on the paper is now destroyed once it leaves the pulping station and cannot be read. Secondly, the pulp is recycled to make other paper products such as toilet paper. So it's good for the environment, too.

How important is the secure destruction certificate you offer?

It's very important because it gives businesses the satisfaction that the documents have definitely been destroyed. It's good for the auditors, showing that the process is transparent and recorded for auditing purposes.

What is coming over the horizon in terms of secure destruction in South Africa? Will the POPI Act influence any changes?

South Africa is pretty new to this kind of legislation, so we are just getting used to it. But it is certain to become more influential as time moves on.

We also see a movement towards digital data, which has already happened in other areas of the world.

The pressure to look after data is already there because people in South Africa are more aware than before. It's going to be more and more important that companies who look after personal data have a data privacy policy and a secure destruction program in place, especially the bigger companies and those who want to grow.

> **Secure destruction of digital data is relatively new here, but it's growing and demand will only increase.**

CHAPTER 3

SECURE DESTRUCTION: A SIMPLE GUIDE STEP BY STEP

Many businesses recognize the value of secure destruction and understand they should not be keeping documents or data indefinitely — both from the point of view of cost and unnecessary risk. But starting the journey takes some planning and preparation.

Here is our step-by-step guide to steer companies through the process, put together by Crown Records Management experts across the world:

1. REVIEW WHAT DATA YOU ARE STORING AND WHY

If you don't generate data in the first place, you don't need to destroy it. So, the very first question to ask is whether the data you are generating is needed or not. Re-engineering your entire data flow can save a lot of money in the long term. This process is a about risk management – which is something we'll come back to time and again. Is the data you are storing valuable enough to warrant the risk associated with it?

2. FIND OUT WHAT INFORMATION YOU HAVE IN THE BUSINESS

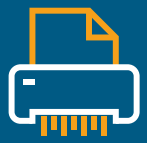
The next step for any business, whether they are storing data onsite or with an outsourced storage and records management company, is to identify what data they have. Do you know what's inside all those boxes? Does every record — physical or electronic, have a retention schedule? Is there any data in storage that is past its retention date and doesn't need to be kept? Data that is being kept unnecessarily, or even illegally, adds dramatically to the level of risk, and that's where a secure destruction policy comes in. Undergoing a comprehensive information audit is a great start and that's something Crown Records Management always offers.

We've seen businesses keep data for 10 years as part of historic policy, not realizing they are breaking the law because some of those records should be destroyed after five years. Then there are others who keep everything indefinitely 'just in case' but have no idea what is being stored or where it is. If they need to find these records as part of a subject access request they are in trouble – and of course they have been paying to store it, too.

If you are storing personal data from anywhere in the world it is vital to understand whether you have permission to do so and how long you can keep it. So an information audit, a retention schedule, and a secure destruction policy go hand-in-hand with lower risk.

3. SEARCH YOUR SERVERS FOR ROT – REDUNDANT, OUTDATED AND TRIVIAL DATA

Boxes in storage are not the only place to search for data being kept unnecessarily. Servers across many businesses are full of data that is being kept even though it offers little or no insight. In some cases, this information is being kept in case it can be useful in the future, but more often because nobody thought to delete it. This might include duplicates because of forwarded emails, print-ups, and home working, but also data which was collected without any purpose. This data does not come without risk. It increases the chances of a data breach, makes systems slower, and costs money and energy to store. If it is not properly labelled, or doesn't have the right permissions, it can also mean companies are breaking data protection regulations. All ROT and dark data should be identified in an information audit and labelled for secure destruction.



4. DECIDE WHAT TO DESTROY AND WHAT TO KEEP

Most businesses decide that there are certain types of documents that don't need to be destroyed – and some that do. But relying on people in the business to do that without a secure destruction policy in place is risky, because people don't always do the right thing. The equation to balance here is the cost of destruction against the level of risk, and this might depend on the type of data generated. Do you aim to be totally safe by destroying everything at source that doesn't have to be kept? For instance, by insisting every bit of paper goes into a secure destruction bin at the office and is then removed by cleaners at the end of the day to be destroyed. Or do you want to focus only on sensitive data or data with a strict retention deadline? There is a cost analysis to make, too. Destroying all physical data is safer but also more expensive; this is something to discuss with your outsourced secure destruction partner. But remember, you can also save money by destroying boxes that cost money to store.

5. TALK TO YOUR SECURE DESTRUCTION PARTNER ABOUT THE OPTIONS

Many companies have found that trying to manage secure destruction onsite themselves brings significant complications, especially if they generate a lot of data. By outsourcing it to experts, they can jointly decide on a policy and service that meet the needs of the business.

6. CONSIDER THE ENVIRONMENT

When it comes to hard drives, there is a big decision to make. It is far better for the environment if they can be reused but this must be balanced against risk. Data can never be completely 100% removed – if a criminal is expert enough, and has the right equipment, they can probably retrieve some of it even after it has been reformatted. They may not be able to get the entire picture, but they can get a lot of information. For highly sensitive data, companies will want the hard drive securely destroyed – but many companies are comfortable with the low risk and with the benefits that come from keeping the circular economy moving. If you have 50 PCs in the office that are out of date and you know they haven't had carried high levels of data (maybe everything is kept in the cloud or on a separate server, for instance) then destruction may not be required. Think instead of donating the equipment as part of your CSR campaign, perhaps to a school. The boost to reputation and the social media content generated are added bonuses.

7. CHOOSE HOW OFTEN YOU DESTROY DATA

This is another decision which balances risk and cost. Destroying data as often as possible is clearly preferable, but also more expensive. It's worth considering that less frequent secure destruction can lead to overflowing bins and herald increased risk – especially if it puts employees off using them. Similarly, a high volume of electronic data can slow down servers, cost money, and increase the risk of data breach. Businesses often like the idea of ad hoc collections rather than paying for a regular slot when bins may not be full – and this has been particularly prevalent during the pandemic. But it comes with added risks and potentially additional cost – because it prevents secure destruction partners from maximizing economies of scale. However, the bottom line is data and documents which no longer need to be kept should be destroyed as soon as possible after their retention date. Saving them all up for a big destruction burst once every year or two may seem cost effective, but it comes with a higher risk.

8. CHOOSE YOUR LEVEL OF RISK

What level of risk are you willing to take with your data? This is a key question when deciding how best to mitigate. At this stage you should be talking to the experts about what type of secure destruction is best for your business and whether it should be done onsite or off. Your secure destruction partner can bring a shredding truck to the premises, or they can collect your data and take it back to a secure facility. It's worth considering how much space you have available. Shredding paper, for instance, increases its volume dramatically, which can create an issue for smaller sites. For highly sensitive data, you may prefer that it doesn't leave the building before being destroyed. Every business is different and there is no right or wrong answer.

9. CHOOSE YOUR METHOD OF SECURE DESTRUCTION

There are many methods of secure destruction and choosing the right one, in partnership with your secure destruction partner, is the next step. The answer is likely to be influenced by cost, by the type of data and by that magic word 'risk'. How big a risk is it to the business if the data ends up in the wrong hands? All methods of secure destruction come with a certificate of destruction and confidence that the data is now irretrievable, but there are parameters. Shredded paper still exists at the end of the process, so for highly sensitive data a business may also want it pulped. Degaussing removes data from hard drives, but some companies will also want the hard drives ground down to dust. There are choices to be made.

10. EDUCATE YOUR EMPLOYEES

Once a secure destruction schedule is in place, it is vital that businesses also educate staff about how to abide by it. What bins should they use? What data must be destroyed and what doesn't? What processes are in place in the workplace? Be realistic, too. If you're expecting employees to walk 50m to put paper records in a bin, the reality is they probably won't do it. Hotdesking is also adding to data risks in terms of personal data left on desks for others to see, so education is required to ensure all data is destroyed at the right time – and that people understand the value and sensitivity of it. This trend may change after the pandemic, but it has been replaced with home working which is just as complex. Education and training are vital. But, of course, the most important thing is for a business is to start their secure destruction journey – before it's too late.

SECURE DESTRUCTION GUIDELINES FROM OUR EXPERTS

ALWAYS APPLY A DESTRUCTION DATE

By Rosena Rabbitte, UK

One of the biggest tips for clients is to always apply destruction dates to any information or data stored.

Not only is it good practice, it also means we can proactively send the client a list of boxes and documents which are going to expire, two or three months in advance. If we know there is a required date for destruction, we can run a list every month. That way nothing need be kept beyond its retention date. It's a very helpful reminder system.

ASK FOR A SECURE DESTRUCTION CERTIFICATE

By Peter Burton, Philippines

It's absolutely vital for customers in Southeast Asia to know for certain their documents or data have been destroyed – so companies should make sure one is issued.

Clients in this region want a full audit trail that proves the documents have been securely destroyed – and they want a certificate that confirms it has all been done. We offer a signed Certificate of Destruction which provides evidence of what has been destroyed, by whom, and on what date. It's suitable for internal and external auditors, including regulatory bodies and government bodies. The client will also be able to show the full history of a box from the time it was first handed over to Crown, including all the retention data for it.

DECIDE WHETHER TO DESTROY ITEMS ONSITE OR OFFSITE

By Kevin Moore, New Zealand

The onsite or offsite debate is one to have with your secure destruction adviser at the start of the project. Both options are available and the decision depends on a company's risk level, budget and size.

Having a secure destruction expert visit your premises is convenient and less expensive. But space can be a problem when there are large amounts of waste to shred.

THINK ABOUT HOW TO TRANSPORT DOCUMENTS SAFELY

By Pieter Nienaber, South Africa

We have a lot of customers who are now working at home but still printing off information. So, one tip is that it's important for them to be able to securely store those documents so that other people cannot access them.

Think, too, about the way you transport information. Carrying sensitive data in your car, or in a hand-held box is not a safe way to transport company data. What happens if you have an accident or if the car is broken into or stolen?

Companies don't always understand that if they take away files or boxes from storage to work at home then suddenly that data is no longer being protected and often there is no process to follow. Businesses need to think about putting those processes in place. Talking to a secure destruction expert can help and they may be able to offer secure delivery options.

CONSIDER THE SIGN-OFF PROCESS IN ADVANCE

By Rosena Rabbitte, Crown UKI

No secure destruction company will destroy any document or data unless it has received sign-off from the client that it can be destroyed. This is a vital safety mechanism but can become complicated if there are multiple people required to sign off the process.

At Crown, clients provide a list of documents to destroy and we put the items on a work order. Once that order has been signed off, it's ready for destruction and then we provide a certificate to show it has been completed.

There are normally 250 lines of destruction on each work order, so if each order must be sent to a different person it can become an administrative nightmare. There could be thousands of them. It's good practice for clients to have a clear sign-off process, preferably with just one department.

HAVE A REGULAR SECURE DESTRUCTION REGIME – DON'T WAIT TO DO IT ALL IN ONE GO

By Peter Burton, Crown Philippines

This is a big issue and one that businesses should think about more carefully. In the Philippines, many banks organize a big secure destruction blitz every two or three years and do it all at once, destroying thousands of boxes at the same time. But the reality is many of those boxes have been kept for too long – way beyond their retention date. If you no longer need to retain data, you should be destroying it as quickly as possible.

For instance, if an auditor asks to look at a box and it hasn't been destroyed then you will be forced to withdraw that box and hand it over – even if it is past its retention date. It's quite possible that potential issues could be avoided by destroying the box on time.

This is one of the many reasons we suggest to clients that data should be destroyed on site under a regular secure destruction program. Once every three years is not enough and not good practice. Every six months is about right.

DON'T FORGET THAT MANY OTHER ITEMS CAN BE SECURELY DESTROYED

By Rosena Rabbitte, Crown UKI

Not everyone realizes that we provide secure destruction services for many other items that are information sensitive for businesses. Paper documents and digitally stored data are the most common, of course.

Company uniforms also hold information. It might be possible for a criminal to use them to gain access to a premises, perhaps.

Some businesses want us to destroy seconds to avoid them ending up on the black market, especially in the fashion market, and others ask to destroy old marketing information. There are a wide range of items which can be securely destroyed to protect a business.

WANT TO ROOT OUT EXPIRED DOCUMENTS? FIND OUT WHEN THEY WERE LAST VIEWED

By Rosena Rabbitte, Crown UKI

One of the most regular questions we get from clients is: can you find out when this box was last viewed?

It's a good question to ask, because by drawing up a list of boxes which haven't been opened for a long time – perhaps even for decades – you may be able to speed up the process of identifying documents which should be destroyed.

UNDERSTAND REGULATIONS OVER SHREDDING ON SITE

By Pieter Nienaber, South Africa

Shredding on site may seem like the most cost-effective way to destroy paper documents but in fact there can be savings made by doing it off-site. No need for any shredding machines or trucks. But some industries in South Africa, especially banks, require information to be destroyed on site so ask an expert to ensure you understand the rules.

Get in touch

Crown Records Management helps clients maximize the value of their "corporate memory" through the storage, active management, and timely distribution of information assets.

In 40 countries, Crown provides secure archiving and retrieval of information in physical and electronic format, as well as digital imaging, media management, and data destruction.

Crown Records Management is part of Crown Worldwide Group, a privately owned, global logistics company founded in 1965 and headquartered in Hong Kong. An extraordinary and purposeful business committed to making it simpler to live, work and do business anywhere in the world.

If you have any questions regarding this whitepaper, email us at info@crownrms.com.

The power of memory | **crownrms.com**

Discover Crown

A complete range of services to help you and your business

crownworldwide.com

- **World Mobility**
- **Relocations**
- **Records Management**
- **Fine Art**
- **Logistics**
- **Workspace**