ITAD BEST PRACTICES

Data Security Services

Author: Josh Feldman
VP Professional Services, Makor Solutions

ITAD BEST PRACTICES

Data Security Services

Author: Josh Feldman, VP Professional Services, Makor Solutions

Data security is serious business. It's also a balancing act. You need to mitigate your customers' liability and provide the highest level of data security services, while maintaining processing volume, maximizing profits and adhering to NAID, R2 and e-Stewards compliance.

"Is there a 'Best Practice' for tracking and servicing hard drives through the ITAD/eWaste/Reseller process?" is a question I hear quite a bit. Having worked with many companies to address this very question, I can tell you the "Best Practice" for your company depends on how you run your business.

Based on insights gained from overseeing almost 70 implementations, I've written this eBook to explain the factors impacting the options you should consider in establishing your "Best Practice" for data security services.

TABLE OF CONTENTS

`

CREATING AN OPTIMIZED DATA SECURITY SERVICE GAME PLAN

To create the best data security services plan, you absolutely must know your customers, staff, warehouse and how you sell. What works for one company will cause bottlenecks or security gaps in another. Here are some key questions you should consider about your business (and why) to help you establish processes that make the most sense for your company.

1. How much transparency/reporting does your customer or compliance body require?

   If you must answer to NAID, R2 or e-Stewards compliance audits or your clients demand reporting, your process must include timely and accurate reporting of services performed. If your client base is less demanding, you still need responsible processes, though you have more flexibility.

2. How many hard drives do you service each week?

   The volume of services significantly impacts where, when and how you service drives and data bearing units.

3. How reliable is your staff?

   Being realistic regarding the skillset and workload of your processing teams and/or individual staff is also crucial in deciding where, when and how you service drives and data bearing units. Do you need to rely more on technical systems to enforce activity or can your team cover the slack and get the job done?

4. Do you have the resources and warehouse space to implement the most ideal process for handling these services?

   The best ideas have to fit your warehouse space and staff availability in order to implement the desired process improvements.

5. How predictable is the volume of incoming computer equipment?

   If you have a predictable flow of inbound servers, desktops, etc., you can better plan the number of hard drives you need on hand versus having to maintain a large hard drive inventory buffer for unknown volume. This could impact your decision to wipe drives in-unit or to remove them.

6. Do you sell more downstream via wholesale or retail channels?

   This has considerable impact on when and how you service hard drives delivered in-unit.

7. Are data security services a revenue stream or just a service you offer?

   If data security services generate revenue, you need to set up processes for the chargeable steps (removal of drives, data collection, wipe/destroy, etc.) early in the process.

8. How do you market/sell your data security processes, if at all?

   Determining how important your data security services are to your customers, in relation to your other services, could impact how you set up your floor. I have worked with customers who created a separate routing process for all potential data bearing devices prior to testing or recycling. They chose to sacrifice a little throughput in order to pitch and market confidence in their process control.

Now that you've done your homework, let's look at some of the most prevalent and/or successful processes to handle onsite hard drive services. Keep your business model in mind as you formulate your plan to set up or adjust your processes.

WHEN & WHERE TO SERVICE LOOSE DRIVES & DATA BEARING UNITS

Servicing Loose Hard Drives

The decision of when and where to handle loose drives is pretty consistent in the industry. In almost all companies, the initial “sorting” team sends hard drives delivered loose to a secure area (or non-secure area depending on business factors) for sanitization or destruction.

For companies with systems in place or capable staff at the “sorting” process, it is preferable to barcode these loose drives and capture data and/or assign services (wipe x1, wipe x3, destroy, etc.) during the initial sorting. This is more efficient than barcoding at the time of sanitization or destruction because of better tracking, ability to bill earlier for services and throughput in the security processing area. The quicker these drives can be recorded and tracked the better.

Servicing Data Bearing Devices

There is a lot of variance in the industry regarding the processing of electronics delivered with hard drives in-unit. Is this process started at the “sorting” area, left to the test/repair technicians or done at an isolated stand-alone process?

Here are some effective approaches to ensure that hard drives are properly handled and that no units go into downstream channels to be sold with customer data — every ITAD, Reseller and eWaste company’s worse nightmare.

Option 1: Removing all hard drives from the unit at "sorting"

Many companies like the predictability and formality of the initial "sorting" teams removing all in-unit drives (from devices where it is feasible to do so).

Pros: Delegates consistent responsibility for the initial step of the data security process to one set of staff resources (*see Loose Drives **above***), captures data and tracks all hard drives at the beginning of the production process and, when a unit is at the tech bench, the system is ready for resale or reimaging within minutes (if replacement drives are readily available).

Cons: Reduces the throughput of the sorting process which could have significant impact on overall productivity and puts data security in the hands of lower tier skillset. Other drawbacks are discussed in the *In-Unit drives: Removing drives or Wiping in-unit* section below.

Some companies remove hard drives while sorting only on devices destined for recycling, leaving the test/repair technicians to handle potential reuse units (see Option 2 below).

Option 2: Servicing data bearing devices at the "test/repair" bench

This seems the most natural choice for companies because of the skillset match, since the device is already being touched and because this is where the diagnostic/data erasure hardware/software is set up to be in service. Just because it's the natural choice, though, doesn't mean it's the best option for everyone.

Pros: Reduces number of touches as services are performed in-line with auditing and testing; increases throughput at "sorting" process; employs a higher skill-set of labor to perform services; doesn't require separate dedicated warehouse floor space; and in many cases, it is connected to the third-party data erasure process.

Cons: Reduces throughput of test/repair process; unwiped drives remain in-unit while in temporary storage longer; and delays tracking.

Option 3: Creating a stand-alone hard drive removal process for data bearing units destined for recycling while sending all potential reuse units to be serviced at test/repair

Companies that don't want to remove hard drives at the sorting process, and don't want to slow down the testing/repair process with scrap, will route data bearing devices destined for recycling to a stand-alone hard drive extracting area.

Pros: Maintains throughput at both the sorting and test/repair benches; improves level of service by formalizing the process of the removal of drives prior to recycling (doesn't leave job to lower tier skillset of teardown staff); having dedicated areas/process flow for your data security services helps market confidence.

Cons: Requires additional warehouse space and personnel; requires extra label printing (units destined for recycle are now being barcoded to tracked security being performed).

Option 4: Creating a stand-alone process where ALL potentially data bearing units are routed to prior to test/repair or recycling

Some companies can rely on their staff or technical systems in place to route potentially data bearing units from their sorting process to a stand-alone data security area. This area is where all drives are either removed from the unit or wiped in-unit prior to going to recycling or test/repair.

Pros: Automated (or manual) routing to an isolated data security servicing area delivers more consistent security services (i.e., less chance for data breaches); produces confidence internally and externally (sales and marketing); and maintains throughput at sorting and test/repair processes.

Cons: Requires additional warehouse space and personnel; may create a bottleneck by slowing the flow of material into the test/repair areas; requires extra label printing (units destined for recycle are now being barcoded to tracked security being performed).

No matter which of these processes you use, without the proper ERP System in place to facilitate an enforced, directed process, your company could be more vulnerable to data breaches.

METHOD TO SERVICE HARD DRIVES

Wipe vs. Destroy

The decision to wipe vs. destroy hard drives is initially driven by your customers. With today's emphasis on reuse and asset value recovery, we see a considerable trend in companies incentivizing their customers to wipe drives. If given permission to wipe or destroy, the cutline varies from company to company based on different factors, including current market value and who they sell to downstream.

Loose Drive Wiping

Many companies are connecting loose drives to a dedicated erasure server with erasure software that displays all connected drives on a single screen for immediate updates of each unit. This allows for simultaneous erasure of multiple drives, while tracking an individual hard drive's wipe status.

In-unit Drives: Removing Drives or Wiping In-unit

The decision to wipe in-unit or to remove and wipe is continually in flux. Companies are experiencing gains and setbacks when employing either option. Almost all companies are currently employing a process that includes a hybrid of both. Here are some things to consider when deciding for yourself:

Why wipe hard drives in-unit

- Removing hard drives from units can be very time consuming (if even possible)
- The difficulty in finding appropriate replacement drives of the same size, form and specifications
- Makes it easier to have units ready for resale without maintaining replacement hard drive inventory
- Facilitates tracking the parent/child relationship (without a proper ERP system)
- Less chance of damaging the parent unit (there are a lot of touches when removing)
- Data security services is completed together with the rest of the job
- No need to maintain part inventory to support removal/installation process (screws, caddies, rails, etc.) for various computer classes and models

Why remove and wipe hard drives

- Wiping in-unit slows down the testing/repair process and, subsequently, the availability of inventory for resale
- If you can adequately maintain a replacement inventory of hard drives (and meet other challenges mentioned above) this may be reason enough to remove and wipe when possible
- Wiping in-unit crowds test benches and takes up warehouse space
- Not limited to number of systems that can be connected to wiping software

Your best option should become clear, depending on your specific scenario and ability to mitigate any of the above challenges.

VALIDATION OF DATA SECURITY PROCESSES

Wipe Validation

It is common practice to verify the effectiveness of sanitization through internal and external audit sampling for data recovery. Validation is done to satisfy R2/e-Stewards requirements, sales/marketing and other internal initiatives.

Internal Validation: Some companies simply verify wipe success manually at completion of each hard drive. Others employ different variances of random sampling using consumer level data recovery software, freeware or other wipe validation techniques on a weekly/monthly basis to ensure proper level of service.

External Validation: Companies where sampling is required for certification or who market their use of sampling to their prospects send a small sampling of wiped drives to a third party audit company on a monthly, quarterly or annual basis.

The need for, method and frequency of sanitization effectiveness verification is dependent on internal factors.

Validation of Overall Data Security Process

Companies employ different methods to verify whether the overall data security process is working and is optimal. Externally, the need for verification is dependent on your customers' demands for transparency and reporting as well as the compliance bodies you are answering to (NAID, R2 and e-Stewards). Internally, factors that drive this scrutiny include ensuring your throughput is optimal, confirming revenue from these services is fully maximized and realized in a timely fashion and verifying your downstream sales team is set up for success (with inventory ready to sell).

The best way to validate your overall process is to employ proper checks and balances and utilize statistics and data to make adjustments. Companies who are best able to validate, correct, improve and maximize their business processes have a proper ERP or warehouse tracking system in place that connects all key business units and processes and includes built-in data security service enforcement and reporting. Analyzing your current processes with fragmented systems, an old, home grown platform that isn't updated frequently or spreadsheets is a daunting task (if even possible). For more on processes, see *Process Enforcement, Tracking, Billing/Reporting and Building Inventory* below.

PROCESS ENFORCEMENT, TRACKING, BILLING, REPORTING & INVENTORYING

Avoiding data breaches, delivering as promised to customers, generating service revenue, staying compliant and making sure your downstream sales team is selling in a timely fashion are all reasons to take your overall data security process seriously. Without the proper tracking of this process, each of these critical goals can be jeopardized.

With this in mind (as noted above) companies are no longer relying on patchwork systems, spreadsheets and old, homegrown platforms to take them where they need to be. The best practice for enforcing process, tracking, billing/reporting and building inventory is to integrate your data security services process with an ERP / Warehouse Management system that connects all key business units (inbound sales to inbound material handling to outbound billing/reporting and downstream selling).

With the right system, this integration should reduce your reliance on the staff and result in:

- Data Accuracy and Known Requirements
  Zero breakdown in the flow of data from one process to the next
- Accurate Services Performed
  Contract enforcement to ensure what needs to get destroyed is destroyed, what needs to get wiped is attempted to be wiped and all needed data is collected
- Increased Throughput
  Integration with data diagnostic/erasure software eliminates extra touches and streamlines data collection and status updates
- Real Transparency, Accurate and Automated Billing/Reporting, and Process Validation
  Track the status of each bar coded hard drive coming through and leaving the warehouse while automatically recording billable activity and compiling reports
- Building of Accurate Inventory
  Successfully wiped drives should be easily checked into inventory for upgrade or resale

IN CONCLUSION

The factors to consider in order to establish your "Best Practice" for performing and tracking data security services should, hopefully, be clearer. Answering the questions posed at the beginning of the article about your business processes, customers, staff, warehouse and how you sell, and knowing your options for each facet of the process will significantly help you facilitate discussions around what is most applicable to your company.

Makor Solutions has been helping customers implement the Makor ERP system, built specifically for ITAD, Resale and eWaste, to integrate their data security process with the rest of their operation to deliver results and advance their business goals. If you'd like to discuss any topics within around best practice for data security services, get connected to companies in your space who've done this well, or explore how the Makor ERP could help, please contact us.

About Makor Solutions:

Makor Solutions has been helping companies in the ITAD, reseller and eWaste industries around the globe streamline and grow their business via implementation of their robust Makor ERP.

About the Author:

Josh Feldman, Vice President and head of the Professional Services team at Makor Solutions, has personally led almost 70 system implementations for some of the most recognizable companies in the industry. With his vast experience in helping ITAD, reseller and eWaste companies optimize material processing, he has witnessed what works and what doesn't. Josh Feldman can be reached at jfeldman@makorsolutions.com with your comments and questions.