Data Destruction as a Service (DDaaS) By Site

TEAR-A-BYTE®

PATENTED PROCESS

tech2

Contents

Page

Introduction: 3
A Move from Loss of Control to Control
Industry Trend – Moving to the Cloud

The Challenges in Data Security 4

Threats to Loose Media 5

Replacing the Old ITAD Model 6

Our Data Destruction Solution 7

The Tear-A-Byte Solution in Detail 8

Data Destruction as a Service (DDaaS) 9

Determine your Requirements and Budget 10

Next Steps 11

A Move from Loss of Control to Full Control

How concerned are you about controlling loose media devices such as mobile phones, tablets and IoT equipment during the age of computer mobilization? Are you still using legacy systems to try to comply with today's difficult requirements? Are you confident that your system will comply with the ever-increasing Audit and Regulatory requirements? Passing your audits is now harder than ever with many questions being asked about your firm's Cybersecurity Framework (CSF) and risk appetite.

How long will the existing Information Technology Asset Disposal (ITAD) industry survive using their outdated processes? Transporting data to centralized collections points in poorly secured vehicles is not best practice and exposes firms to risk. Using non-compliant transport techniques is just one part of the problem. Most facilities do not meet datacenter security requirements. Anyone holding data for months before destroying it is exposing themselves to unnecessary risk. Modern Risk Management best practices require custody of devices through their lifecycle. Anything deviating from this does not meet federal and state Cybersecurity regulations.

Wherever you are in the process, we can help. This whitepaper will describe the steps to get your company to the top industry solution for media destruction.

Industry Trend – Moving to the Cloud

Moving your data to the cloud sounds easy enough, but as a Data Owner, you will now have to implement policies and systems so that you maintain control of your data. The hard part of your job is to lead your operations, security, and compliance teams and help them keep data secure in those environments.

While cloud providers are responsible for the security in the cloud, the responsibility for the data bearing media is ultimately yours. Just as you need to secure the devices stored in your on-premises networks, so you need to secure the equipment in the cloud environment. Many leaders are confused about the concept of the distribution of ownership, which results in widespread security gaps in implementation of cloud management.

Cloud computing is quickly changing the operating model for small to large firms. Michael Zanga, Managing Director East Coast TechR2, led many migrations of data when he was working in the client arena. Michael Zanga provides this explanation:

"Consistent operations across internal systems and cloud-based systems are imperative. The firm is still the data owner regardless of how the infrastructure is delivered."

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

The Challenges in Data Security

Whether you are moving to the cloud or maintaining your own datacenter, media security is still paramount when protecting your data. The ever-growing internal threat is when media is loose. It is not tracked, it is not contained, it is not properly destroyed under your control, and worst of all, it is not verified.

During the life of data storage equipment, there is maximum security. In a datacenter, there is an outer security fence (the first perimeter), the building exterior (the second perimeter) and a separated secure interior area (the third perimeter) that isolates data from all those who should not have access to your data. In some datacenters, there are secure door requirements on server racks (the fourth perimeter).

What perpetrators know is that on any given day, when a device fails or needs to be decommissioned, many companies lower their shields to the first security layer and the data on the loose media leaves their control and goes out the door of the building.

To confront this challenge, we offer a solution that meets every data security regulation worldwide.

To confront this challenge, we offer a solution that meets every data security regulation worldwide.

- We **Track** your loose media inventory utilizing Cloud based Asset Management software
- We **Contain** your loose media in a steel vault assembled by ISO 9001 certified manufacturers
- We **Destroy** your loose media using NSA certified tools
- We **Verify** the entire process onsite to ISO and SOC standards

100% of this process is done onsite, environmentally soundly and safely under your control and at maximum security.

Most importantly, this solution is essential in cloud datacenters, where you are not present. When moving data to an external site, your responsibility to control the data bearing devices moves there as well. When your Service Technicians work onsite to replace failed devices, they now have a place to enroll and secure loose media.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE TECHR2 IS NIST COMPLIANT MBE Ohio Achieve GDPR COMPLIANCE ZERO TRUST MODEL

201-05/24

Threats to Loose Media

Just as organizations enjoy the automation benefits that datacenters offer, cyber criminals do also. Today's cyber attackers increasingly infiltrate datacenter environments and take advantage of the fact that an impersonator will not be recognized by datacenter staff.

IBM estimates the data loss in physical breaches as a result of unauthorized access at $400 billion annually.

The risks of unauthorized access to data are reported as:

- Risk One: The Insider Threat
- Risk Two: The Outsider Threat
- Risk Three: The Seemingly Innocent Personal Item
- Risk Four: Poor or Nonexistent Identity Verification

These startling results highlight the frequency with which cybercriminals are targeting cloud-based datacenters using simple techniques that breach security. The challenge for security teams lies in identifying and securing potential vulnerabilities and stopping attacks in their tracks. Security needs many layers, and numerous tools are being implemented across enterprises to protect the data in motion.

What is being done when it is at rest on an End of Life (EOL) device?

Maintaining compliance standards

The most astonishing element to arise from cloud datacenters and the advent of IaaS, PaaS, and SaaS (Infrastructure, Platform and Software as a Service) is that they have impressive compliance credentials, but they only accept the external security and power responsibilities for the data center. If you check their security policies that are HIPAA or ISO approved, they also declare that data and media security inside the environment is your responsibility. Regardless of how the data is served from a provider to a client, the responsibility for security is not outsourced.

Another weakness in the existing data security infrastructure is that OEM Cybersecurity Compliant manufacturers have impressive arrays of credentials. The majority of the IT support companies do not. If you send out a request for ISO 27001 or SOC-2 Cybersecurity Framework certificates from these companies, you will receive nothing. They have decided that data security is not their priority.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Data Destruction as a Service (DDaaS)

Replacing the Old ITAD Model

Although the old guard of data security reviewers recommended to you on their websites that you could utilize the Old ITAD Model, it just is not so. That model is dead.

In the world of Cybersecurity Frameworks (CSF) and Risk Management, you will be fined for jeopardizing your data security and likely lose customers, especially when following Old ITAD institutions that tell you that you can bypass data security measures.

Ignore the myths and choose the new solution that is compliant to standards that are accepted globally in a world economy.

Here's a comparison:

Old ITAD Model

- Transport data in a cardboard box to their facility
- Any repair technician can walk out the door with customer data on the media
- They will not be held contractually bound to protect the data in transit
- They do not need a Cybersecurity Framework certificate
- They will not issue a Certificate of Destruction (CoD) to NIST standards
- They do not have to use a Sanitizer and a Verifier
- Any video camera can sign the Verifier signature on the CoD

HDR Plus TAB

- Track your loose media onsite with TAB
- Contain your loose media onsite with TAB
- Maintain control of the media within the four walls of the datacenter
- The media destruction company is ISO 27001 certified and NIST 800-171 compliant to DFARS standards
- The Certificate of Destruction (CoD) provided meets NIST standards
- Two technicians, a Sanitizer and a Verifier, arrive onsite to destroy the data to standards
- The US Patent office found that a video camera cannot act as a Verifier signature

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Data Destruction as a Service (DDaaS)

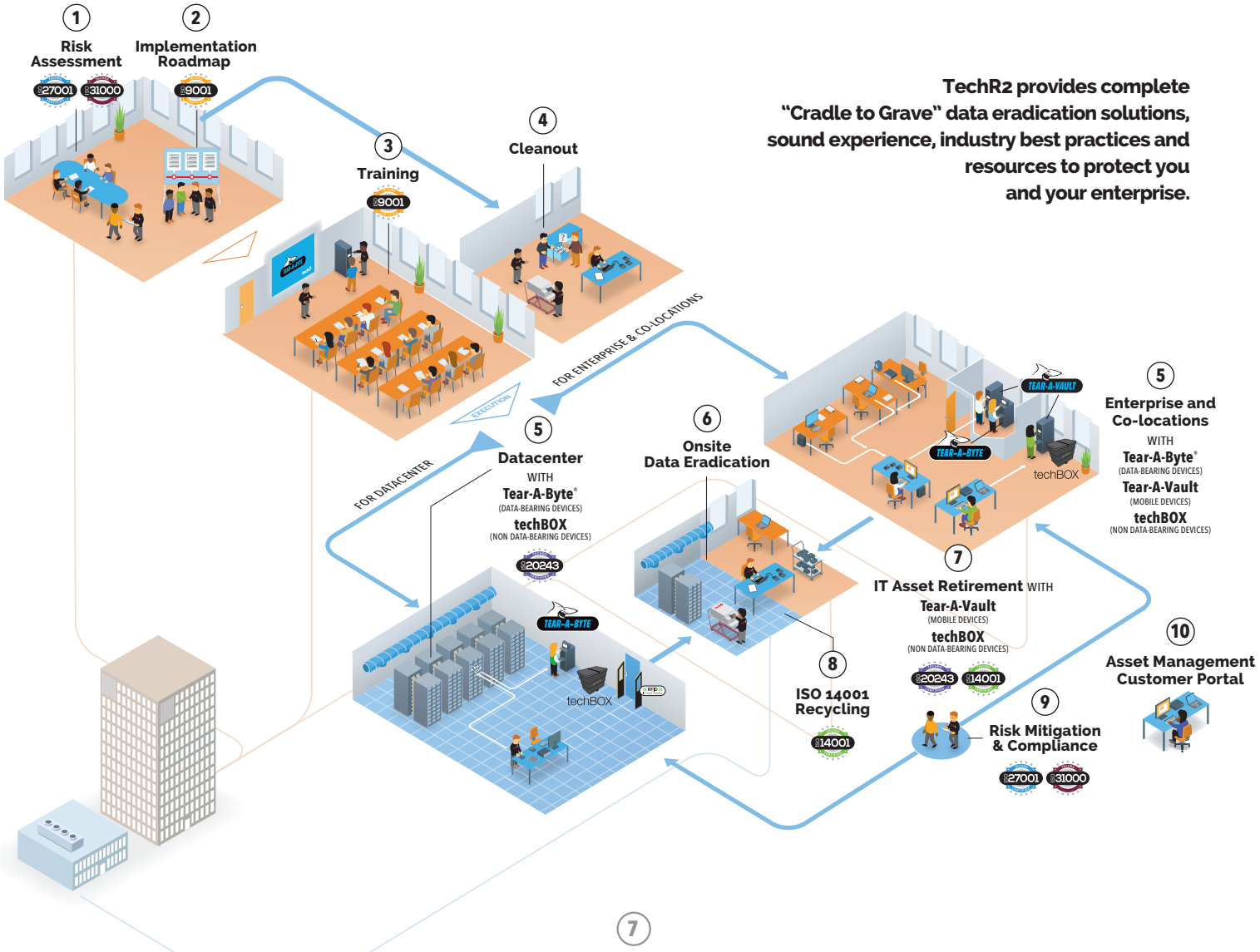
techr2.com **614.322.2222**

Our Data Destruction Solution:

The TechR2 patented Tear-A-Byte® solution

Includes:

- Compliance to NIST SP 800-53, NIST SP 800-171, HITRUST, HIPPA, PCI, NERC, FERPA and other Cybersecurity requirements
- Meets Zero Trust Architecture requirements
- Annual Risk Assessment at the Tear-A-Byte Site
- Free IT Asset Recycling at the Tear-A-Byte site using TechR2 Secure techBOX® Containers
- Integrated Training at the Tear-A-Byte Site
- Green Reports for Environmental Responsibility
- Legal Certificate of Destruction (Sanitization)
- Audit Reports are on 24-7 Customer Portal



TechR2 provides complete "Cradle to Grave" data eradication solutions, sound experience, industry best practices and resources to protect you and your enterprise.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE | TECHR2 IS NIST COMPLIANT | MBE Ohio | Achieve GDPR COMPLIANCE | ZERO TRUST MODEL

Data Destruction as a Service (DDaaS)

- Track
- Contain
- Destroy
- Verify

1 1x Event

TechR2 performs a risk assessment to fully identify risk for data at rest and check compliance to industry and federal regulations.

2 1x Event

A plan is created to secure the datacenter and all loose data bearing devices throughout the enterprise. Customer's also go through a brief training session on using Tear-A-Byte®.

3

The process begins with RFID tagging each device for real-time tracking and inventory control. The secure Tear-A-Byte® appliance receives and contains each device. For retired assets that do not contain critical data, the SMART techBOX™ offers containment-to-disposal management.

4

Once filled to capacity, TechR2 Security Engineers and the customer are notified via the proprietary TechR2 Customer Inventory Management portal. Our Security Engineers are then dispatched and arrive onsite at a conveniently scheduled time.

5

TechR2 Security Engineers verify and destroy all media onsite using NSA and DoD approved technology and processes after capturing, auditing, and reconciling the data bearing device. Security Engineers double verify the reconciliation process to ensure a successful process.

6

After approval of the onsite report, the client receives a Certificate of Destruction, Environmental Report and a detailed Audit Report via the TechR2 Customer Inventory Management portal.

TEAR-A-BYTE® PATENTED PROCESS
By TechR2
Enterprise & Datacenter

It's patented!

Additional Services

- Datacenter Decommissioning
- End Of Life Cleanout
- Risk Assessments
- Retired Asset Services

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE | TECHR2 IS NIST COMPLIANT | MBE Ohio | Achieve GDPR COMPLIANCE | ZERO TRUST MODEL

Data Destruction as a Service (DDaaS)

Data Destruction as a Service (DDaaS)

Patented Tear-A-Byte® in the Datacenter

At the datacenter and enterprise office sites, our partners will be equipped with the Tear-A-Byte® Appliance(s) of the appropriate size, inside the four walls of security to Track and Contain failed or decommissioned data bearing devices. When a media device such as hard drive, data tape or mobile phone fails, your onsite technicians will use the Tear-A-Byte Appliance kiosk to record the serial number, manufacturer name, model number and where the device was attached as well as the technician name and date-time stamp of when it was deposited after receiving a Tear-A-Byte RFID tag. Once the Tear-A-Byte Appliance is filled, ISO 27001 certified TechR2 will send two technicians onsite to reconcile, destroy, and verify destruction within the four walls of the company site. The Track, Contain, Destroy, and Verify patented Tear-A-Byte process meets NIST SP 800-171, NIST SP 800-53, NIST SP 800-88, ISO 27001, and PCI requirements as noted in your Cybersecurity Framework (CSF).

Accompanying your Tear-A-Byte Appliance inside your company site, a TechR2 SMART techBOX secure container will house the tech equipment that no longer holds any data. Your company technicians can add RFID tags to servers and IT equipment and place them in the secure container. Utilizing the Tear-A-Byte and SMART techBOX solution in tandem provides clean and organized datacenters devoid of the typical IT equipment accumulation. When the techSMART BOX is filled, it will be shipped to TechR2 for ISO 14001 recycling.

Hub Consolidation Site using Patented Tear-A-Byte®

Some of your company's smaller remote sites have fewer data bearing devices such as laptops, tablets and IOT equipment. Identified company hubs can be equipped with Tear-A-Byte and SMART techBOX containers, and your company can use Secure Transport Services to move enrolled devices from the origin point to the hub site without violating the NIST Cybersecurity Framework (CSF).

Company hubs will have at least a 42U or a 22U Tear-A-Byte Appliance inside their four walls of security to Track and Contain failed or decommissioned data bearing devices. Hub technicians will use the Tear-A-Byte Appliance kiosk to record the serial number, manufacturer name, model number and where the device was attached as well as the technician name and date-time stamp of when it was deposited after receiving a RFID tag. Once the Tear-A-Byte Appliance is filled, ISO 27001 certified TechR2 will send two technicians onsite to reconcile, destroy and verify destruction within the four walls of your company site meeting the NIST Cybersecurity Framework (CSF).

Your company technicians can add RFID tags to servers and IT equipment and place them in the secure container. Utilizing the Tear-A-Byte and SMART techBOX solution in tandem provides clean and organized datacenters devoid of the typical IT equipment accumulation. When the SMART techBOX is filled, it will be shipped to TechR2 for ISO 14001 recycling.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE TECHR2 IS NIST COMPLIANT MBE Ohio Achieve GDPR COMPLIANCE ZERO TRUST MODEL

Data Destruction as a Service (DDaaS)

Determine your Requirements and Budget

It is a simple process to bring ISO level compliance to your media destruction needs. Answer these questions.

1. What is the number of datacenters (TABs)? _____
2. What is the number of consolidation points (TABs)? _____
3. What is the number of enterprise offices (TABs)? _____
4. Total number of TABs (add lines 1, 2 and 3 from above) _____
5. Estimate the number of failed and decommissioned devices per year (average from the last 3-5 years of ITAD processing) _____

Locate the number of failed and decommissioned devices in the first column (yellow color) that matches your answer in question 5. Pick the column color that matches the number of Tear-A-Byte® (TABs) you need from line 4. Your monthly subscription rate is shown below the estimated annual piece count.

Example of sample pricing. For exact numbers, contact a TechR2 Representative

		Datacenter, Hubs and Office TABs		
Annual Data Bearing Devices (DBDs) Processed	**Frequency on Site**	**1 to 5**	**6 to 10**	**11 to 15**
0 to 27,000 DBDs (quarterly visits)	Quarterly	9000 pcs	18000 pcs	27000 pcs
	Monthly Subscription	$14,708	$29,417	$44,125
27,001 to 54,000 DBDs (8 visits a year)	8 Visits per Year	18000 pcs	36000 pcs	54000 pcs
	Monthly Subscription	$19,208	$38,417	$57,625
50,000 to 100,000 DBDs (monthly visits)	Monthly	33300 pcs	66600 pcs	99900 pcs
	Monthly Subscription	$26,183	$52,367	$78,550

Added Value

Recycling is included, at no additional charge, using a leased secure SMART TechBOX™ container for a 90-day turnaround of IT equipment without data at every Tear-A-Byte® location.

- Online Inventory of Data Assets Tracked (RFID Tracking)
- Annual Risk Assessment at the Tear-A-Byte Site by ISO 31000 and ISO 27001 Certified TechR2
- Integrated Training at the Tear-A-Byte Site from ISO 9001 Certified TechR2
- Green Reports for Environmental Responsibility (See sample attachment A)
- Legal Certificate of Destruction (Sanitization) (See sample attachment B)
- Audit Reports on 24-7 Customer Portal (See sample attachment C)

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Data Destruction as a Service (DDaaS)

Next Steps

Moving from your own datacenter facility to the cloud is the current industry trend. Network architects need to take into account that data bearing devices will fail or need decommissioning. That is when your data control solutions become paramount to avoid breaches.

Next steps are:

1. You should have an End of Life ISO 31000 Risk Assessment completed for the datacenter to examine policy and procedures to your Cyber Security Framework.
2. Update your cloud datacenter policies and procedures to the current regulations. Distribute the polices and provide training.
3. Select a CSF compliant third-party solution to support the datacenter's CSF.
4. Follow up with annual Risk Assessments to make improvements.

Contributing Authors

Sepp Rajaie
CEO and President, TechR2

30+ years Executive Level Management
Visionary Entrepreneur
Patent Holder
Cyber Warrior

Charles Robbins
Senior Compliance Officer, TechR2

43+ years in Software and System Development
Retired Infantry and Armor Officer
Prolific Author and College Teacher
Cyber Warrior

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**