techr2

Achieving Compliance in Data Storage Security

Upholding the highest industry standards

ISO 27001 ISO 31000 ISO 9001 ISO 14001 ISO 45001

techr2 Media Security Solutions. **techr2.com**
48 Klema Drive N., Reynoldsburg, OH 43068 | 614.322.2222 | clientrelations@techr2.com

TEAR-A-BYTE PATENTED PROCESS

An IBM Exclusive Global Supplier

Achieve GDPR COMPLIANCE

176 10-19

Contents

Achieving Compliance in Data Storage Security

How successful are you at securing data in a diverse environment? Are you trying to make outmoded network systems compliant? Do you have confidence that you have control of the data you possess?

Maybe you did survive another year where the internal compliance auditors did not ask the hard questions. Will you endure through the harder compliance audits being launched this year by federal and state agencies?

How long can you hide the facts that your current processes are not tied to Cybersecurity regulations concentrating on Risk Management, Planning, Training, and Compliance?

Wherever you are in the process, this whitepaper can help you. It explores the nine steps in securing public and private data in your internal networks and on the cloud, giving you real world solutions that are resilient and evolve with you.

This paper also includes threat assessments from IBM and TechR2.

Moving your data to the cloud sounds easy enough, but as a Data Controller, you will now have to implement policies and systems so that all of your Data Processors are compliant. 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 public cloud providers are responsible for the security in the cloud, the responsibility for the data is ultimately yours. Just as you need to secure the data stored in your on-premises networks, so you need to secure the data in the cloud environment. Many leaders are confused about the concept of the distribution of ownership, which results in widespread security gaps in implementation.

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

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

The Challenges in Data Storage Security

Given the simplicity and cost-effectiveness of the public cloud, it is no surprise that more and more organizations are turning to the cloud for data storage. You can meet the power and external security requirements without expending large amounts of capital.

While the public cloud solves many traditional IT resourcing challenges, it does introduce new headaches. The secret to effective cybersecurity in the cloud is improving your overall security posture: ensuring your architecture is secure and configured correctly, having the necessary visibility into your architecture, and most importantly, who is accessing it.

While this sounds simple, the reality is anything but simple.

The rapid growth of cloud usage has resulted in a fractured distribution of data and its control. Even worse, the technicians handling your data at the cloud facility are not at your facility, they are not adequately screened by your team or by the cloud datacenter and even worse, when maintenance is being performed, the IT equipment leaves datacenter without satisfactory control.

Lack of data security leads to both compliance risks and breaches.

Monitoring exposure

The need to oversee the cloud datacenter operation by adding a system to control data is paramount to managing these environments effectively. Ticketing systems, firewalls, and servers are all integral segments of the network system.

Surprisingly, when moving data to an external site, the responsibility to control the data bearing devices moves there as well.

Threats to personal and public data

Just as organizations enjoy the automation benefits that the internal networks and cloud datacenter offers, cyber criminals do also. Today's cyber attackers increasingly infiltrate datacenter environments and take advantage of the fact that their 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[i] 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 sophisticated techniques. The challenge for security teams lies in identifying and securing potential vulnerabilities and stopping an attack in its tracks.

With the General Data Protection Regulation in affect, the risk of having stockpiles of data tapes and hard drives is causing companies to implement "GDPR Purges" to regain control of their data management.

"GDPR has expanded the responsibility of protecting critical data to any entity that is a 'controller' of the data," says Sean Gouhin, EVP and Corporate Counsel at TechR2. *"As such, traditional Chain of Custody concepts will no longer protect an organization from regulatory reach."*

Maintaining compliance standards

The most astonishing element to arise about cloud datacenters is that they have impressive compliance credentials, but they only accept the external security and power responsibilities. If you check their policies that are HIPAA or ISO approved, they declare that data security inside your cage is your responsibility. Not theirs.

Nine Steps to Compliance

Step 1: Governance and global mandates

The EU General Data Protection Regulation[ii] (GDPR) that went into effect on May 24, 2018 has changed the landscape of data protection for tracking.

Article 33 and Recital 85 require controllers to notify the supervisory authority of a personal data loss no later than 72 hours after having become aware of it.

Article 25 and Recital 87 state that it should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place.

Cybersecurity Framework (CSF) Compliance is required for companies doing federal work.

The Federal Acquisition Regulation (FAR) governs all federal government acquisitions and contracting procedures; DFARS is the special supplement for DoD-related contracts. The FAR Final Rule 52.204-21 on "Basic Safeguarding of Contractor Information Systems," which became effective June 15, 2016, contains 15 controls that are considered the minimal baseline for federal contractors. These controls resonate with basic security objectives contained in NIST SP 800-171 Revision 2.

Starting this year, the compliance model will begin to move from self-attestation (i.e., the current NIST SP 800-171 compliance model) to third-party validation in accordance with the new, five-level Cybersecurity Maturity Model Certification (CMMC).

The majority of US States adopted the NIST Cybersecurity Framework (CSF), specifically NIST SP 800-53 R4 for their agencies, contractors and subcontractors. Media Protection (MP) is one section of the NIST CSF that has been scrutinized by the US Inspector General for failing the control.

NIST SP 800-53 MP-6(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Industry rules require businesses to be subject to mandatory compliance standards imposed by the government (such as HIPAA, SOX, PCI DSS). These standards often stipulate how businesses should secure Personally Identifiable Information (PII), and other sensitive data. A Data Loss Prevention (DLP) policy is a basic first step to compliance, and most DLP tools are built to address the requirements of common standards.

HIPAA requires strict control of medical data which eliminates the possibility of shipping loose media and decommissioned data bearing devices offsite.

FFEIC Handbook Rules for Banks and Financial Institutions require extraordinary tracking and containing of data and data bearing devices.

Payment Card Industry (PCI) - Credit card processors are required to notify the card associations on a quarterly basis to identify any merchant who is not PCI compliant. Merchants can face penalties and fines by the credit card associations for not being compliant and may even have their ability to accept credit card payments terminated.

IBM Own Cloud Compliance Policy

Compliance - Last Updated: 2019-07-31

IBM® Cloudant® for IBM Cloud provides a trustworthy and secure cloud database system. The service is built on best-in-industry standards, including ISO 27001:2013.

HIPAA - IBM Cloudant, when deployed on dedicated hardware on IBM Cloud, meets the required IBM controls that are commensurate with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rule requirements.

International Organization for Standardization (ISO) - IBM Cloudant and IBM Cloudant Dedicated Cluster are audited by a third-party security firm and meet ISO 27001, ISO 27017, and ISO 27018 requirements.

SOC 2 Type 2 Certification - IBM provides a Service Organization Controls (SOC) 2 Type 2 report for Cloudant.

General Data Protection Regulation (GDPR) - The GDPR seeks to create a harmonized data protection law framework across the EU and aims to give citizens back the control of their personal data, while imposing strict rules on those hosting and 'processing' this data, anywhere in the world.

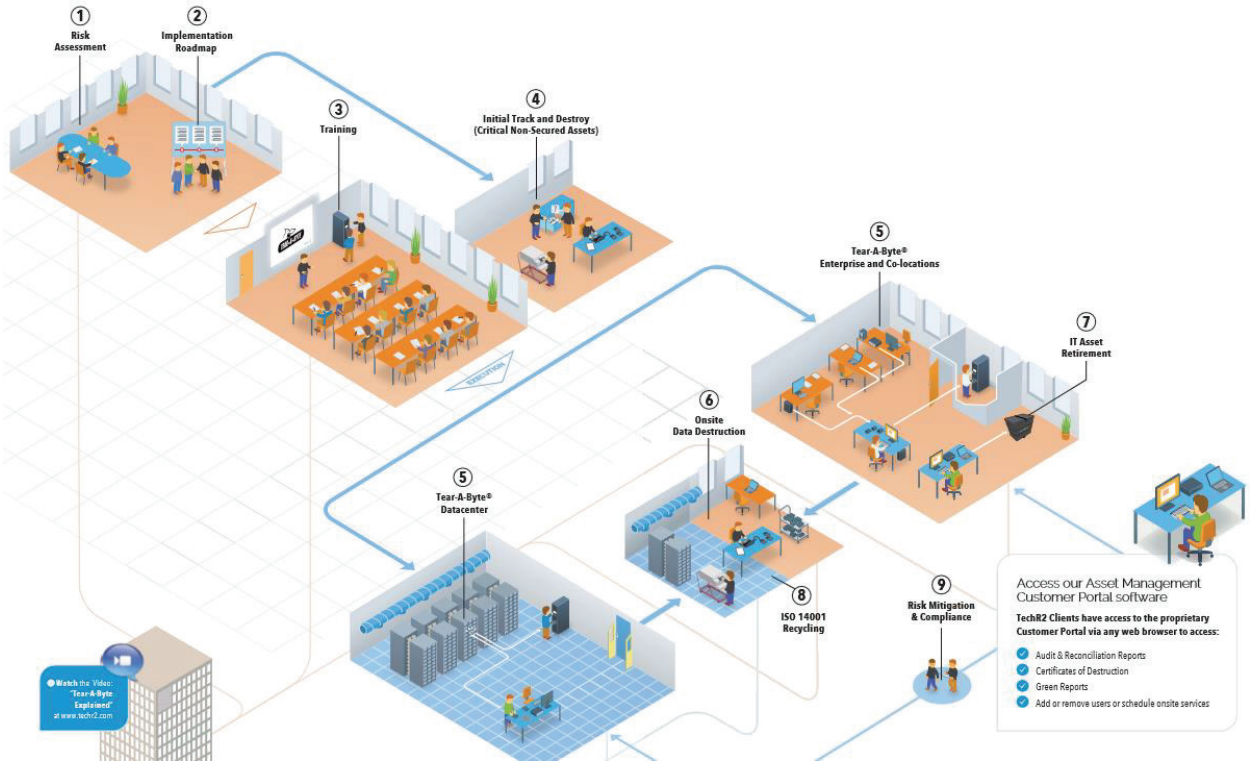
Step 2: Plan for multi-step processes

You will find that Cybersecurity Frameworks (CSF) follow logical data security steps to Identify, Protect, Detect, Respond and Recover. Control of your data in a cloud datacenter is part of this multi-step sequence.

1. Complete a Risk Assessment to determine current status
2. Receive Implementation Roadmap to move towards and update compliance
3. Customer receives data security training
4. Install Security Appliances
5. Security Appliance utilization by staff
6. Destruction Event with reconciliation, audit, destroy data, Certificate of Destruction (CoD) and ISO 14001 recycling
7. Close Project and transmit CoD, Audit and Green Reports, and Certificate of Recycling

Step 3: Global view

You need data control that is a cradle to grave solution for tracking, containing and destroying Data at Rest and is a proven technique used by large financial, healthcare, retail and hospitality industries. The solution should a far right and far top choice in data security and helps you pass your internal regulatory audits, since the solution is fully compliant and certified for ISO 27001, 9001, 45001, 14001 and 31000.



Step 4: Follow Track – Contain – Destroy – Verify

By now, you should be aware of the Federal and State NIST CSF requirements that require you to control the data in the cloud datacenter. You must:

- Track your data-bearing devices using a technological method such as RFID and establish a real time inventory and audit trail via tailored customer portal.
- Contain data-bearing devices securely in a locked Appliance, only accessible by certified staff.
- Destroy data onsite, within the four walls of your facility, and receive a Certificate of Destruction prior to the departure of the dual technicians.
- Verify data destruction via dual controlled teams and electronic reporting to reconcile internal data bases/asset inventories.

Step 5: Automate your processes

When a company experiences a Data Security incident, which solution do you think a CISO wants? A completely digital solution that actually meets the NIST SP 800-88 R1 regulation or a something someone locally just contrived. Look at your Certificates of Destruction and compare them to the NIST standard and you will be shocked that your old solution is not compliant.

Besides compliant reports, your data security team will appreciate the ease of conducting internal audits on your systems without the necessity of flying to each location. Your internal auditors can view current data 24-7 through a Customer Portal.

Step 6: Accept ISO and worldwide compliance

It is 2019 and non-compliant data security companies are selling their products and services to you. How do you separate those third-party providers who will cause you to fail your audits from those who will not? Innovation in solving your problems is number one. Proof of cybersecurity compliance is the next.

The ISO compliance system is your way to know that the data security, quality management, environmental services, health and safety, and risk management programs are internally and externally audited to worldwide standards.

Step 7: Environmental acceptance

Responsible technology recycling is essential for end-of-life data bearing equipment. Improper disposal can lead to fines, litigations, and most importantly a data breach. But such disposal is more than mere self-protection — it is a moral imperative. Your recycler should lead the charge to honor the environment. Your research, your expectations, and your reactions to changes in data and environmental law and practice may affect you — operationally, financially, and ethically.

Your recycler should keep a vigilant eye on the global business and environmental culture so that you are better able to understand and fulfill your role while maintaining optimum value. As stewards of the environment and a student of sound business practices, your choice should develop strategic alliances with organizations that share your environmental goals.

Step 8: Make the Cybersecurity transition

In the coming years, companies and their third-party providers must all comply with Cybersecurity Framework (CSF) programs. Where most companies in the world are not compliant, those who take data security seriously for their clients have held their CSFs for many years.

Step 9: Grow your security

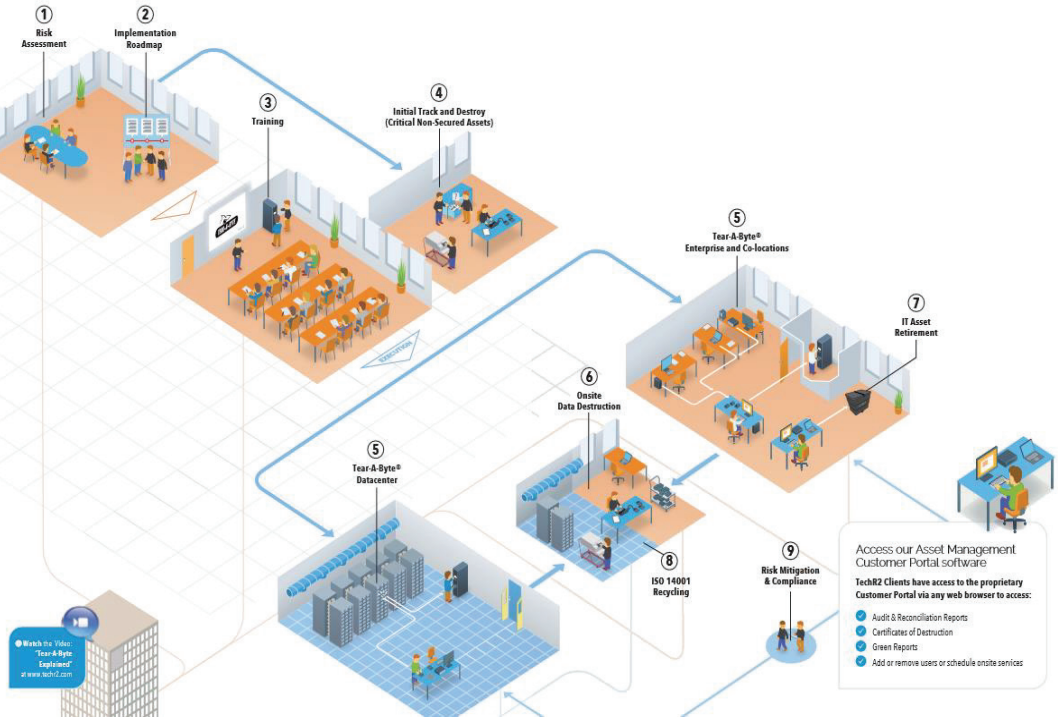
As part of any Cybersecurity Framework (CSF) program, annual Risk Assessments, Planning and Training will create a multi-layered data security program that will also inspire growth in your other data security programs. You know that you cannot stay at the status quo. Data security is either growing or failing. Partnering with world-class data security professionals will enhance your program.

TechR2 Introduces the Tear-A-Byte® Solution

Data Eradication

Data Eradication is the process of removing information from media to protect the organization that is in possession of it and the client who provided it and has the rights to the information. Both entities must meet governmental regulations that mandate data security. Although an organization may have a customer annotate an agreement when they provide personal, medical, or financial data, the persons handling the information have the responsibility to ensure that the data does not fall into another's possession as a data breach, which can cause harm to the customer. This concept is backed up by governmental regulations which mandate that all organizations protect the data under their control and that they must follow procedures that show acquiescence to the rules. In the end, whatever techniques we utilize for protecting and eliminating the data, we need to follow a logical sequence that guarantees compliance with the regulations.

Although there could be a multitude of different kinds of systems utilized to perform data eradication, there is a logical sequence of events reflected in this patented Tear-A-Byte® method that guarantees compliance. We will discuss the logical sequence of events for the Tear-A-Byte® Method which are shown as follows:



1. Perform a Risk Assessment
2. Implement a Roadmap
3. Conduct Training
4. Initial Track and Destroy
5. Perform Tear-A-Byte in the Data Center
   Perform Tear-A-Byte in the Enterprise and Co-Location Sites
6. Onsite Data Reconciliation and Destruction
7. Execute IT Asset Retirement
8. ISO 14001 Recycling and Zero Landfill Policy
9. Evaluate the Risk Mitigation and Compliance

After this introduction to the data eradication process, we should note that the Tear-A-Byte® Method is a comprehensive solution. It does not rely on a specific tool or software application that may work for the short term or for only a part of the data security requirements. We believe that data will always exist on some kind of media, and professionals are needed to perform data eradication that is in compliance with regulations and protects customers and their clients.

Risk Assessment

The first step in the sequence begins with a risk assessment, where we discuss and record all of the objectives that need to be accomplished for data eradication. This type of document is required by governmental regulations and industry guidelines, so managers and professionals should become well educated in the practice. Within the realm of management, we use the document to measure our strengths and weaknesses for planning, execution, and evaluation. For professionals who have to execute the data eradication plans and receive a written score, we want to meet or exceed industry standards and create a plan for data security that is innovative and designed for your specific needs. We can utilize existing risk assessments, but eventually we want to adopt one that is specific for your application using our diverse methods for the solution.

The team approach to conducting the risk assessment is the best technique to use where we do not leave any stone unturned. Managers, professionals and support workers should be included in the process. This is our direct team. Indirect team members such as third-party providers, maintenance staff, and insurance agents should be consulted, so we are aware of all your organizational requirements. This will result in the creation of an authentic preliminary score and development of a plan to reduce your risk.

In an internal or external audit, an organization can receive a passing or failing score in any area that relates to the risk assessment. Failing scores are most likely to be seen on external audits. Industry surveys across the western world show that managers and professionals who are responsible for internal audits do not know the real time status of their data bearing devices and may score the risk as low on any requirement when the data could be or actually is going out the door. As managers, professionals and support employees, we may feel overwhelmed by the information reviewed in a risk assessment, but a good defense against risk begins with an honest evaluation. Anything less than 100% commitment at the beginning of the process will make the risk assessment incomplete and may not provide plans needed for the organization's data security improvement.

We believe we can categorize the risk assessment into logical groups to help consolidate our thoughts for pertinent outcomes. These groupings are:

1. Control of Data Bearing Devices
2. Destroying Data from Loose Data Bearing Devices
3. Training of Personnel
4. Disaster Recovery Planning and Training
5. Budget Planning
6. Auditing

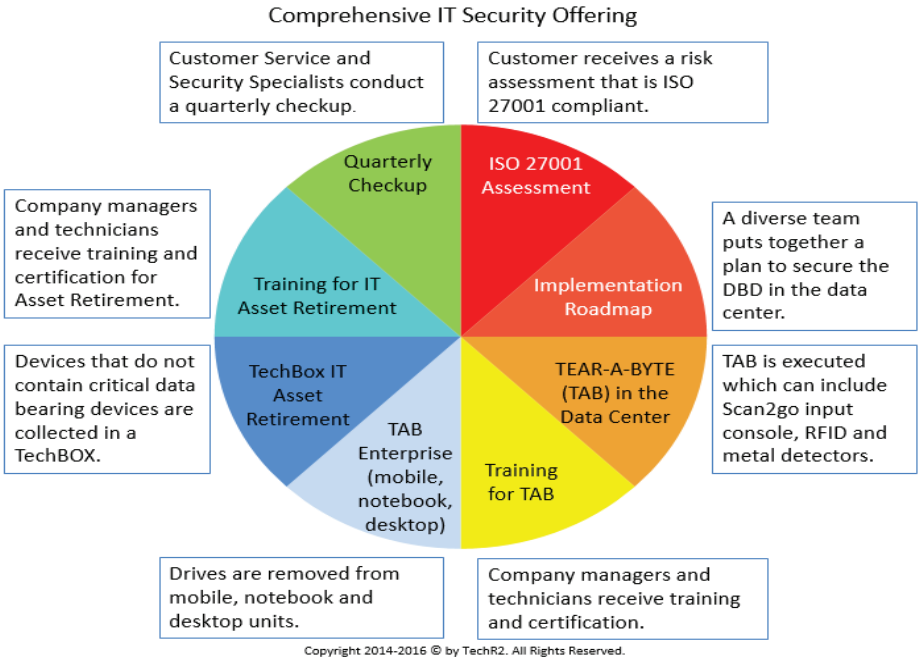
For assessing risk, we perform risk identification, risk analysis, and risk evaluation using scoring and rater comments for the requirements addressed in each grouping. After the risk assessment documents have been completed by all those participating, a comprehensive report is written and provided to you in a follow-up meeting. This report includes a review of all items on the risk assessment, a risk assessment ranking, review of evaluator notes for strengths and vulnerabilities, and the plan with recommendations developed for your organization to address your specific needs.

Implementation Roadmap

After the Risk Assessment and Analysis, our Implementation Roadmap begins and focuses on all facets of security. It includes regular evaluations. Other evaluations are scheduled if needed due to identified security concerns. Following each Risk Assessment and Analysis, an updated Implementation Roadmap begins based on the results of that assessment.

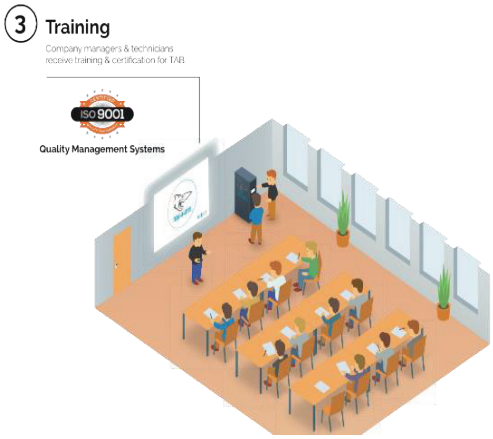
Across all cybersecurity regulations, we implement a real security solution that involves:

1. Tracking of the all data bearing devices
2. Demonstrating onsite containment
3. Maintaining all data bearing devices on your premises, since shipping critical devices to another location jeopardizes customer data
4. Each datacenter and satellite location need a written plan for data destruction
5. Managers need regular reports to prove they are tracking data bearing devices
6. Companies need regular training on handing failed and decommissioned devices
7. Internal or external audits conducted that shows compliance



Conduct Training

TechR2 provides training for company personnel who will enroll failed or decommissioned data bearing devices into the Tear-A-Byte Appliance. This training is accomplished using webinars, videos and step by step manuals. We then verify the training has been completed by testing technicians' knowledge to the 90th percentile for certification. We then provide the company with reports of their training status, which are given directly to their managers.



This vital training step is easy to implement by adding the TechR2 training program link as part of your company's training package.

Tear-A-Byte training is conducted:

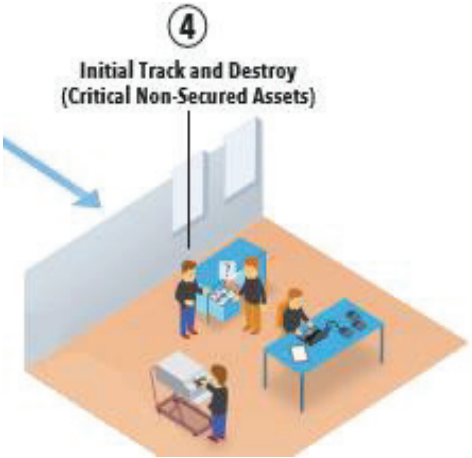
- Online – using webinars, videos, audio and step-by-step manuals.
- TechR2 trains managers and technicians to the 90th percentile for certification.
- Company receives certification report for compliance records
- Real time reports and notifications of training are provided

Training is also included on the Tear-A-Byte® Appliance kiosk through the "tutorial" option.

User education is a key component of making security a more distributed model. Michael Zanga Managing Director East Coast TechR2 says *"All users inside Technology and out, play a part in protecting a firms data front to back. It is not enough to look at it from a privileged access perspective alone. TechR2 has demonstrated success with our Risk Assessment process identifying gaps that were previously unknown and really made a difference for our valued customers."*

Initial Track and Destroy

During the Tear-A-Byte® Risk Assessment, we can locate loose media in the Datacenter, Enterprise office, and, if necessary, in the Co-Location sites. These units contain intellectual property along with customer and environmental data of every kind. For many years, the low number of data breaches has not prompted any serious reactions in many data centers. Now data breaches are announced regularly for many companies, from the smallest to the largest.



As the number of data bearing devices (DBDs) increases in amount and extends greatly into all areas of our professional and personal lives, we need control of their whereabouts, or we will need to accept the fact that we will be losing data and to expect data breaches as a part of our digital landscape. These loose data bearing devices are immediately locked down and we schedule a clean out.

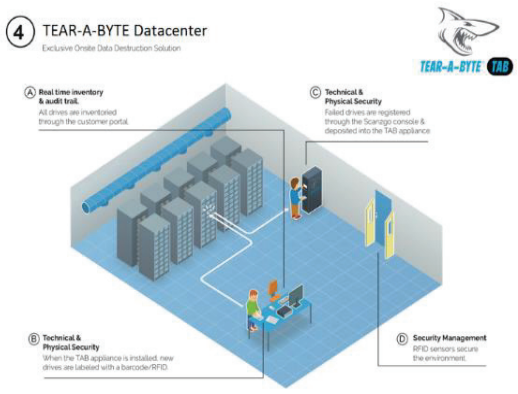
Therefore, we provide the procedures, the equipment, the training, and the certified personnel to track, contain, destroy, and verify data on your DBDs and conform to governmental regulations and industry standards. When completed, we give you an authentic Certificate of Destruction that meets the NIST 800-88 guidelines.

Tear-A-Byte® finds Critical Non-Secured Assets

- Non-Secure Assets are discovered during the assessment
- Non-Secure Assets are tracked, contained, destroyed, and verified
- Management has real time reports and notifications that the clean out was completed to information security regulations

Perform Tear-A-Byte® in the Datacenter

Enrollment and containment of failed or decommissioned data bearing devices in the datacenter is accomplished with the TechR2 42U tall, 600 mm wide and 800 mm deep Tear-A-Byte Appliance. We place the metal 42U Appliance permanently inside the datacenter. This step provides the best security for controlling those data bearing devices once they are removed from their server. No other approach that we have seen or tried has come close to this security measure. Construction of the 42U Appliance is by ISO 9001 manufacturers, and the appliance easily holds four hundred 3.5 SAS hard drives in their caddie. Our kiosk has an easy 1-2-3 step enrollment application where we capture detail information from the person depositing the hard drive, date and time of enrollment and the serial number of the device.



TechR2 datacenter 42U Tear-A-Byte® Appliance:

- Made by ISO 9001 certified manufacturers
- Each Appliance module holds up to 400 – 3.5 SAS hard drives in a caddie
- Kiosk to facilitate simple enrollment of data bearing devices
- Managers can view contents of the appliance through the TechR2 Customer Portal
- Managers can easily set notification parameters to control maximum device count

Tear-A-Byte® in the Enterprise and Co-Location Sites

For the enterprise office, TechR2 provides a 22U tall, 600 mm wide and 800 mm deep Tear-A-Byte Appliance. By placing the metal 22U Appliance permanently inside a designated and secure room, we automatically have the best security for controlling those data bearing devices once they are removed from their laptop or desktop computer. Construction of the 22U Appliance is also by ISO 9001 manufacturers, and the appliance easily holds two hundred and fifty 3.5 SATA hard drives. The kiosk mounted on top of the appliance has an easy 1-2-3 step enrollment application where we capture detail information from the person depositing the hard drive, date and time of enrollment and the serial number of the device.

TechR2 Enterprise 22U Tear-A-Byte® Appliance:

- Lower profile appliance made for the office environment
- Made by ISO 9001 certified manufacturers
- Each appliance module holds up to 250 – 3.5 SAS hard drives
- Kiosk to facilitate simple enrollment of data bearing devices
- Managers can view contents of the appliance through the TechR2 Customer Portal and can easily set notification parameters to control maximum device count

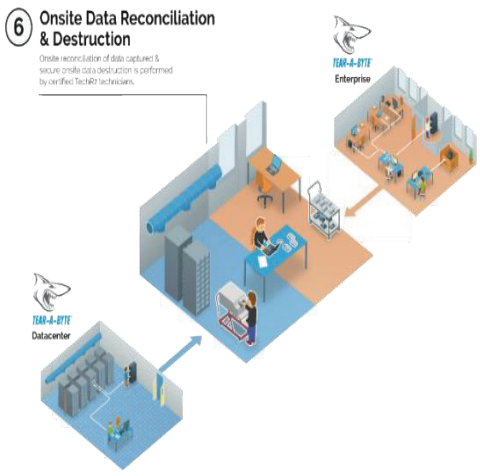
TechR2 10U Rack Mount Tear-A-Byte® Appliance:

Our smallest unit is the 10U 19-inch rack mount Tear-A-Byte that is perfect for co-location datacenter sites where it can be mounted and locked into one of your own server racks. Construction of the 10U Appliance is also by ISO 9001 manufacturers, and it can easily hold fifty 3.5 hard drives.

- Rack mount for co-location datacenter sites
- Made by ISO 9001 certified manufacturers
- Each appliance module holds up to 50 – 3.5 SAS hard drives
- Kiosk to facilitate simple enrollment of data bearing devices
- Managers can view contents of the appliance through the TechR2 Customer Portal and can easily set notification parameters to control maximum device count

For all Tear-A-Byte® Appliances, managers can view audit summaries and even detail information of the past and present audits from the TechR2 Customer Portal. They can add and remove users as well as schedule onsite services while seeing their quarterly reviews and annual assessments.

Onsite Data Reconciliation and Destruction

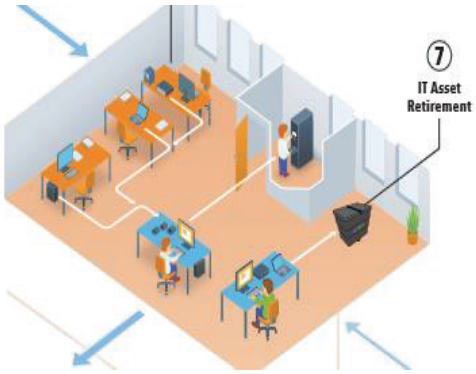


TechR2's secure data eradication methods are tailored to be performed inside the four walls of the datacenter as opposed to allowing any possibility of the DBDs leaving the building. We are so confident in our process that we applied for and were granted a US Patent in 2016. This patented process also uses a two-person team to prevent collusion. It is compliant with the assessing, planning, training, tracking, containing, destroying, evaluating and the auditing clauses of data eradication regulations. The Tear-A-Byte processes are environmentally sound. TechR2 technicians will properly destroy the data on each device and then the e-waste equipment will be processed to international standards. Enrolling devices with a unique identification tag, reconciling what is being processed, and verifying the destruction of the data bearing devices are all part of the TechR2 patented method. These unique practices provide for cradle to grave data security that is backed by our insurance policy.

TechR2 is second to none in data destruction methods

- Holds top data eradication US Patent
- Uses regulatory sanitizer and validator per NIST regulation
- Process and Documentation is compliant with:
  - GDPR
  - NIST SP 800-88 R1
  - NSA
  - HIPAA
  - FFIEC
- Onsite process is clean and environmentally

IT Asset Retirement

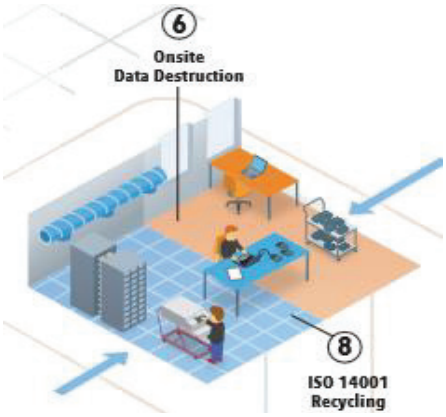


TechR2 also offers a wide range of IT Asset Retirement solutions for their customers that is anchored on their secure data destruction methods. Many customers use the TechR2 secure techBOX® to transport servers, computers, laptops, monitors, printers, and network equipment to our safe facility for ISO 14001 processing after the data bearing devices are removed from the equipment by the customer's trained IT team or TechR2's IT team.

For company refreshes, TechR2 technicians will properly destroy the data on each device and then the e-waste equipment will be processed to international standards. TechR2 is ISO 14001 certified and honors a zero-landfill policy.

ISO 14001 Recycling

The Tear-A-Byte processes are environmentally sound. For Onsite Data Destruction, TechR2 technicians will properly destroy the data on each device and then the e-waste equipment will be processed to international standards. TechR2 is ISO 14001 certified and honors a zero-landfill policy.

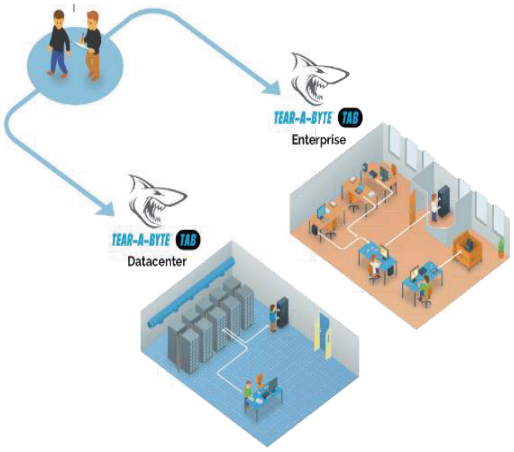


TechR2 services include:

- ISO 14001 Recycling
- Environmentally safe recycling of e-waste

Risk Mitigation and Compliance

TechR2 solves the challenges CTOs, CISOs and IT Managers have regarding efficiently and accurately destroying data on a wide range of platforms. TechR2 has the experience, knowledge, and the technical aptitude to meet any customer's requirements. TechR2 provides Certificates of Destruction that have legal standing. We issue quarterly checkups with quantitative summary and scorecard for each audit. We update your risk assessment and communicate to the managers and technicians if retraining is needed. We provide Green Reports showing that the e-waste was processed environmentally and safely. As you know, data security is evolving to counter known threats, and you need a data security team that is agile and innovative. That is TechR2.



TechR2 will provide:

- ✓ Certificates of Destruction that have legal standing
- ✓ Quarterly checkups
  - Quantitative summary
  - Audit scorecard
- ✓ Update to the Risk Assessments
- ✓ Manager and technician retraining if needed
- ✓ Green Report showing the e-waste processed environmentally and safely

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 cloud 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 cloud 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

Michael Zanga, Managing Director East Coast, TechR2
24 years Executive Level Information Security Officer
Quality Management System Expert
Certified Information Systems Security professional (CISSP)
Cyber Warrior

Sean Gouhin, Executive Vice President, TechR2
26 years Executive Level Management
Legal Counsel
Cyber Legal Subject Matter Expert (CL-SME)
Cyber Warrior

Charles Robbins, Senior VP, Chief Data Protection, Risk Mitigation Officer, TechR2
42 years in Software and System Development
Retired Infantry and Armor Officer
Prolific Author and College Teacher
Cyber Warrior

Upholding the highest industry standards

ISO 27001 ISO 31000 ISO 9001 ISO 14001 ISO 45001