Q1: We already have a process.

Answer: Does your process meet the current regulations such as GDPR (May 24, 2018 launch) or NIST SP 800-53 and NIST 800-88. The NIST requirements are called out in the NERC sanitization guidelines for the power industry.

Q2: What are the basic requirements of the data sanitization process?

Answer: Data sanitization is covered by Federal NIST, Financial, Health (HIPAA), Utility (NERC), Publicly traded (FFEIC and NIST), Retail (PCI/DSS), and GDPR (European). All of these have a common thread. Control of the data.

Q3: Does compliance / risk know that IT is sending data bearing device out the datacenter?

Answer: In most cases datacenter workers touch the data bearing devices but are not given the authority to risk the corporation's money. The risk compliance department sets that standard and we find they choose not to lose control. Basically, they do not know the IT department is sending the data outside the datacenter. Once they discover that fact, they change the IT department policy to not let the data leave the datacenter.

Q4: What other companies know about the 4 walls data security rule?

Answer: Amazon datacenters destroy the data bearing devices onsite. So do the Microsoft Azure datacenters. IBM needs to stress their system guarantees that equal security.

Q5: When has compliance caused IBM to change their process?

Answer: HDR rolled out in the last decade so that customers had control of their data. That control is mandated in each industry and federal NIST regulations. Because NIST is called out in federal law, a company can be fined for giving their data to another company who does not contractually guarantee that the receiver will be responsible for the breach.

Q6: What article of GDPR is IBM and TechR2® Tear-A-Byte?

Article 87 of the GDPR says 'it should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject.' The IBM Tear-A-Byte solution is a tracking – containing – destroying – verifying method.

Q7: What makes TechR2® different than others?

Answer: TechR2® always does the work inside the datacenter. TechR2® uses two technicians where others use one. TechR2® Certificate of Destruction reports meets compliance regulations and others just give a serial number. TechR2® tracks and contain the data bearing device while others put the drive in a box or back room.

Q8: Will IBM's delving into the Media Destruction Industry uncover weaknesses?

Answer: Yes. In every interaction in TechR2®'s region, executives and compliance officers are happy to report that this uncontrolled and unmanaged process has been given a cohesive solution. In many cases, at companies, each individual site was doing their own thing.

Q9: How big a problem is a lack of control in data security?

Answer: Data security specialist have agreed that the internal threat is still the number reason for data breaches. Cisco reported that tracking critical assets reduced human error and standardized the process.

Q10: We do not have to meet any requirements?

Answer: At a minimum you have to meet industry standards and the US, it is the NIST standards. They are complex, and IBM HDR with Tear-A-Byte are already meeting them. It is the standard that your company will be measured against when you have breach.

Q11: What is my company loses a hard drive and does not report it?

Answer: First, if you do not have a method to track and contain loose media, you would never know if you will lose anything. A perfect example is when an IT person takes a hard drive from a turned off storage server to use elsewhere when they need a hard drive. IBM and Tear-A-Byte removes the possibility of hard drives and data tapes lying around.

Q12: Why does a company need two technicians to destroy data?

Answer: The two technician requirement is called out in NIST 800-53 and 800-88. These two guidelines are called out in nearly every other law, regulation or government contract for data destruction. The sanitizer destroys the data and verifier certifies the work by visual or scientific test. During the TechR2® patent process, the video tape verification method used by others was found not valid to allow for a signature.

Q13: What is different today than ten years ago?

Answer: There are many types of data bearing devices, so there is not one method for data destruction in the industry. So IBM and Tear-A-Byte has methods that are appropriate for each type of device.

Q14: Why is shredding unhealthy to humans?

Answer: Shredding and crushing done safely and to OSHA standards is safe, but as you know, shredding truck drivers and technicians do not wear the safety equipment you would see in a factory. TechR2® has found college students running these machines and they were never told about safety procedures and e-waste dangers. The CDC and the State of California has made similar reports about shredders.