Data Security and Decommissioning in a 5G and Streaming World

SEM®

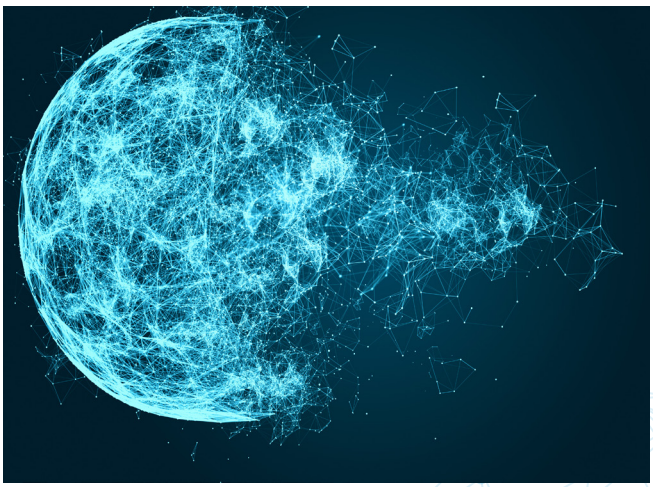
Global Leader in High Security Information End-of-Life Solutions for Over 50 Years

“Welcome to the future.”

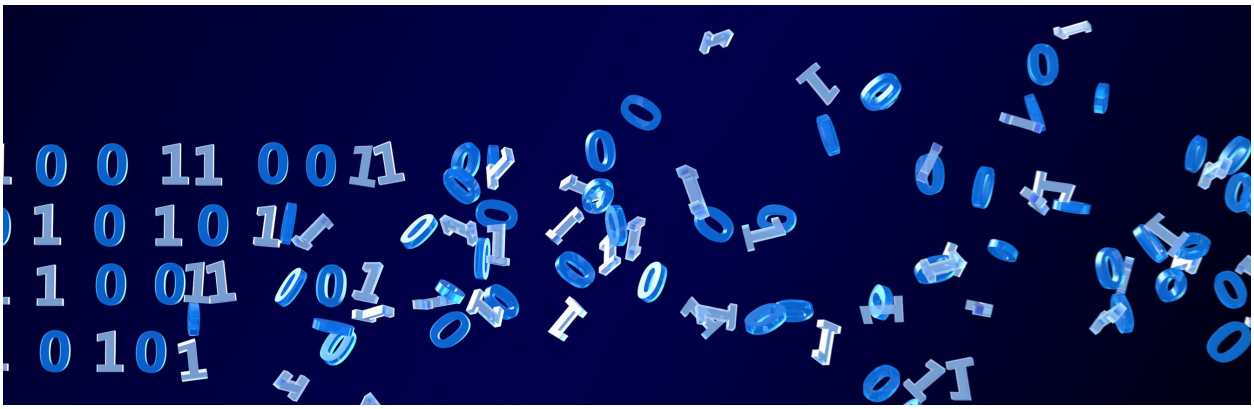
These are the words that will echo off of PowerPoints in executive meeting rooms, organically growing through a marketing machine that ensures that customers know that the latest and greatest of technological advancement is here. Data, which is constantly in a state of change itself, is about to have a brand-new canvas from which it is shared, stored, and consumed. The next generational data network, 5G, has long been establishing its foundation that will be built upon for years to come, and the industries that this affects will start to engage in the necessary changes to take advantage and keep up with the latest tech.

The transition from 4G to 5G networks will be transformative to the way consumers are able to access their data. The speed of web browsing will increase. Streaming data from movies, TV shows, games, and music will see an increase in speed, graphical fidelity, and more. Enthusiasts will start to target 8K video over 4K. Denser data will be uploaded, downloaded, and shared at greater speeds and in more places than ever before.

Streaming alone has seen tremendous growth over the last decade, before 5G was even in the conversation. Now, every day it seems that new players are ready to jump in to pursue and push the latest in streaming technology. Disney and Apple recently joined the streaming service war alongside Netflix, Hulu, and Amazon Prime Video, with Disney+ and Apple TV+, respectively. Sony, Microsoft, and Google are beginning to implement and expand new streaming platforms for video games in an industry that until very recently was largely consumed by dedicated physical hardware. Music streaming also continues to be as popular as ever, with Spotify and Apple Music raking in millions of subscribers, including 217 million subscribers for Spotify alone.



That’s a lot of information to send and receive. And that’s *only* entertainment.



5G will also usher in a new era of interconnectivity between smart objects. Smart cars that communicate with each other and traffic signals will be on the road in a few years. Smart houses with incredible interconnection will be controllable from cell phones and watches with little to no latency. On an even larger scale, entire cities will now have the tools at their disposal to make interconnected smart communications that can monitor systems in real time with these increased speeds and low latency.

For consumers of digital media and content creators, this 5G rollout is exciting news. For businesses that store and handle data, however, this transition will present some costly, high security risk challenges. One often overlooked risk in the digital age comes in the form of data disposal and destruction. With the growing threat to cybersecurity, where an attempted attack happens every 39 seconds, physical end-of-life destruction is often treated as a less immediate concern. The fact is that the improper disposal of physical media can lead to devastating effects to government entities, individual companies, organizations, and consumers.

Who needs to worry about this? Well, chances are, almost everyone. The US government's data, consisting of top secret, classified, and Controlled Unclassified Information (CUI) among others, will eventually see its storage replaced. The general public's information, including health care records, bank information, and additional Personally Identifiable Information (PII), is also stored on physical media. Even if these industries store this information locally, more and more businesses and organizations are hiring cloud services to store their data off site in large commercial data centers owned by the likes of Google (Cloud Services), Amazon (AWS), and Microsoft (Azure). These data centers are where the physical destruction of media will matter the most, as hard drive disks (HDDs) and solid state drives (SSDs) are replaced with new, more technologically advanced counterparts on a regular basis.

Data Centers: Staying Ahead and Staying Secure

As the 5G rollout continues, data centers will find themselves scaling to reach the coverage and speeds that are provided. The more data being delivered to consumers, the larger the drives and data centers that store the data need to be. This means that the transition from 4G to 5G will have two definitive results: new data devices with an increased capacity of storage allowing more information, and construction of entirely data centers that will be able to reach previously low connection areas that are now covered by the 5G network.

Updating Existing Data Centers

Existing data centers are presented with the challenge of not only maintaining the data that is housed, but also keeping the technology used to store that digital information up to date. In the largest data centers around the world, there are upwards of 10,000 individual drives that make up the storage of just one single location. These numbers, while large, barely compare to the total amount that large data providers actually house across all of their locations globally. Not only do those locations hold all of the hosted data, they also store multiple copies of all of that data as a failsafe. So, when the decision is made to start the process of replacing drives, it can be a timely, cost consuming project.

Replacing now obsolete devices can also be a risk for a company, as replacing data allows for more chances of data leakage. That is why it is imperative that, when these drives are replaced, they are also safely and securely physically destroyed, ensuring complete confidence that no data leaks or breaches can occur. Data breaches have been on the rise in the United States over the last decade, skyrocketing from 157 million recorded data breaches in 2005 to over 1.6 billion through 2017. These breaches can result in large fines, a destroyed public image, and a loss of income that can take years to repair, with some companies struggling to ever recover.

That recovery is a wound that is very difficult to heal, because once a breach happens, it's not an easy fix. A lot of time, money, and persistent effort has to be executed by an organization to earn an affected consumer base's trust back; whether that means literal time and effort by the breached organization's employees, or money and time spent in PR management, crisis services, and marketing communication to try to change the consumer's perception of the organization. Some organizations have a lot of cash on hand and will be able to survive the hit and move forward, but for others, a hit to public perception and consumer data loss could spell

the end for their business. In fact, 60 percent of all small businesses that are affected by a data breach go out of business within just six months.

Every precaution should be taken to avoid a data leak or data breach, which is why security experts stress the importance of both cybersecurity and physical end-of-life destruction. So, when data centers begin the process of replacing large quantities of storage drives in a data center, what is the correct method of disposing of the physical media that is being replaced?

The safest method to physical destruction is to have end-of-life data destruction machines on-site at data centers. By having equipment on-site, a data center can control who internally has access to the drives and ensure that they are only handled by vetted employees. Third party companies exist that offer off-site destruction, but when it comes to housing the amount of information that data centers hold, it is both more cost effective and secure to limit the number of people involved.

Different industries have different, specific regulations that dictate how physical media must be destroyed based on the information that is on it. For example, per NSA standards, rotational hard drives that house top secret data need to be both degaussed with at least a 2.0 tesla electromagnetic pulse and then physically destroyed, ensuring that the drive can never be used again or have any data recovered from it. Other industries that have their own regulations are the payment card industry with the Payment Card Industry Data Security Standard (PCI DSS), the healthcare industry with the Health Insurance Portability and Accountability Act (HIPAA), the financial industry with the Fair and Accurate Credit Transaction Act (FACTA) and the Sarbanes-Oxley Act (SOX), and in Europe, the General Data Protection Regulation (GDPR) affects all businesses that operate and handle data of a citizen of a European nation, whether said business is European or not. Therefore, it is crucial that organizations know these regulations.

Building New Data Centers

The demand for faster and denser data will ultimately drive the creation of brand new data centers to aid in storing and moving the colossal amount of data consumed by companies and consumers. As these new buildings are constructed, data disposal procedures may not be at the top of the list of concerns because the technology used during construction will be as modern as it can be. But replacing drives does not only occur when they become obsolete, but when they have an error and fail as well.

In a data center housing thousands and thousands of drives, a certain number of drives are guaranteed to fail due to mechanical or electrical error. This is nothing out of the ordinary, as all mass-produced technology has an expected margin of error when it comes to the construction and shipment of these products, added with the fact of the stress on these drives by running 24/7. Anticipation of these failures shouldn't be an afterthought when constructing new buildings, and if they don't yet exist, a data destruction decommissioning policy should be drafted that informs data center employees of the proper procedures to destroy the data at end-of-life.

By having a proper data decommission policy, three focus points can be established that will aid in the security of housed data for years to come: routine, accountability, and security. By having a set of instructions through a data policy, new employees can be trained to follow a specific routine of what to do with old, damaged, or obsolete data. Systems can also be put into place that allow accountability, such as having a specific storage area for devices waiting to be destroyed and another specific area where the destruction is always done, with both areas requiring a security code or badge scan to access.

Security is the most important. A strict data decommissioning policy protects the employee, the data center, and the company whose data they store from any leak or improper handling from the randomness that can exist without clear processes. No drive will be left in a box, on a desk, or just thrown in the trash when it is explicitly stated what the policy is and the risks and damage that can occur when not followed correctly.

It cannot be stressed enough how detrimental a data leak or breach can be if it occurs. As stated previously, data leaks destroy companies. Having a data decommissioning policy in place can help cast a safety net over a data center and its employees to mitigate unnecessary risks. No two data policies are the same, and it is crucial that a data center researches both the necessary regulation requirements and machines that would be compliant to meet the volume of the data center.

These Changes Will Take Time

Large technological changes take time. There is no master switch that just needs to be turned on, but instead years of preparation, planning, and implementation with continued years of updating and support. The transition from 4G to 5G will bring faster speeds, lower latency, and smarter objects that consumers will incorporate into their daily lives, but it will also increase the amount of data that is shared daily. Data centers will inevitably be adjusting and scaling thousands of locations around the world to meet these needs through new technologies and new locations.

It is critical for companies to acknowledge and address the security challenges that these changes will present as old media is replaced, and having a proper plan and policy will be crucial to a secure transition. Establishing the necessary industry regulations and having compliant data destruction equipment on-site can eliminate unnecessary risk and reduce the chances of a data breach or leak. Planning now can protect the future of consumers, data centers, and individual companies that host their data in data centers as the transition to the future begins.

Andrew Kelleher
President & CEO
Security Engineered Machinery

Security Engineered Machinery Co., Inc.
5 Walkup Drive | Westboro, MA 01581
800.225.9293 | 508.366.1488
contact@semshred.com
www.semshred.com