FIVE WAYS TO IMPROVE YOUR SECURITY DURING IT ASSET DISPOSITION (ITAD)

WHITE PAPER

SIMS LIFECYCLE SERVICES

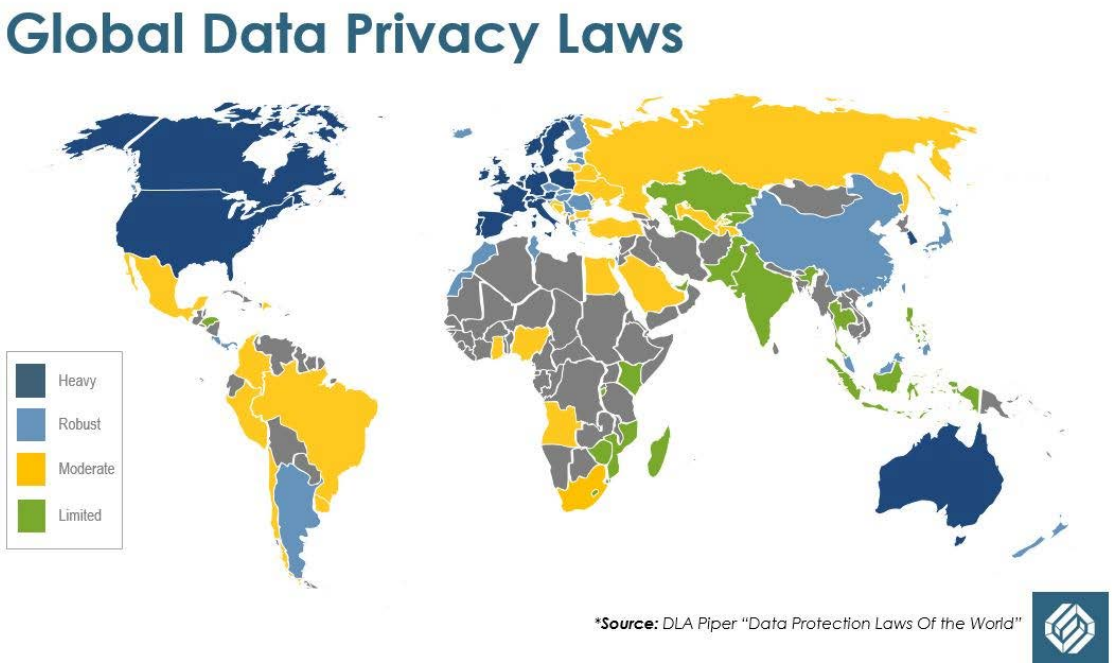
It’s always in your best interest to protect data stored on IT assets, whether working or not. Data stored within servers, hard drives, mobile devices and other IT equipment could exist even when you thought you had it all removed.

In this evolving environment IT leaders continuously need to understand new requirements for data protection.

Europe acted toward unifying data protection with the introduction of a single law, the General Data Protection Regulation (GDPR). This law came into force in May 2018 and provides structure for businesses anywhere in the world to securely collect, store and use personal information of European Union citizens.

California passed a digital privacy law, the California Consumer Privacy Act (CCPA) in 2018. When compared to the GDPR, the CCPA takes a broader approach on what constitutes sensitive data. This privacy law provides consumers with the right to know what information companies might be collecting about them and why and requires companies to remove and dispose of data per consumer request. Virginia, Colorado, Utah and Connecticut have subsequently introduced their own legislation, taking effect throughout 2023.

The development of data security regulations is largely driven by the growing awareness of existing data threats and risks. More businesses today are aware of the damage a data breach can cause. According to E-scrap news, one global bank's IT disposition errors have cost them over $163 million.



> **81%** of consumers would stop engaging with a brand online after a data breach.

Third party vendor relationships can expose organizations to data risks. Before contracting with suppliers who will have access to IT systems and personal information companies are carefully considering potential data privacy and security concerns. Contracting processes increasingly involve extensive due diligence through detailed vendor questionnaires and contracts which include data privacy provisions, end of contract stipulations and specific data protection agreements.

Today's businesses are focusing on ramping up their cybersecurity and, understanding this, data thieves may try to search for the less-common security gaps where there may not be as much resistance. Security gaps often overlooked are those that exist during IT asset disposition. Fortunately, there are steps you can take to ensure that those gaps are filled during the disposition of your IT equipment.

1. Confirm data wiping is executed properly.

Various options for data wiping exist and there are programs that can be purchased, or companies specialized in IT disposal who can do this for you. If done correctly, data wiping procedures are generally 99.999 percent effective, a percentage acceptable for the U.S. Department of Defense, the German Federal Office for Information Security (BSI) and the UK HMG Infosec Standard No. 5.

While performing this task in-house can be a convenient and more cost-effective solution, the statistic holds true only "if done correctly". To ensure verifiable data destruction, outsourcing this service is recommended. This is especially true for companies in need of wiping a large volume of servers and hardware. Work with a vendor capable of supporting ongoing updates as well as fail-safes for scenarios where the wipe is unsuccessful. It's essential to know that the chosen vendor continues to improve their systems and processes for today and for the future. It is also critical that the disposition vendor has operational excellence to ensure nothing will slip through the process.

2. Review the security of equipment during transit.

As cargo theft rises, electronics (and the data they may contain) are becoming increasingly vulnerable throughout the transport process. In a 2020 report, electronics ranked second as most targeted by thieves, and this doesn't take into consideration the value of any data stored. With a variety of solutions for data wiping the first step is getting the equipment safely to the facility so these services can be conducted. Internationally there is an association setting a standard for secure transportation referred to as the Transported Asset Protection Association (TAPA). The certification available through TAPA is important to note. A physical examination of the transportation process, however, is the best approach to ensuring your equipment will arrive safely.

It is important to point out that when a vendor drives away with your retired IT equipment this doesn't mean the risk is removed. If a company's laptop or a server is stolen from a truck and data is exposed, the company, not the transportation vendor, is liable for any implications of data exposure.

It is always recommended to have vehicle security measures in place appropriate to the nature of your equipment and data.

3. Verify asset tracking and facility surveillance.

While it is important to ensure secure transportation of IT assets it does not just end there. The next step is making sure all items will remain secure once they arrive.

Security and tracking of IT assets while they are processed at the vendor facility is important for a few different reasons. The security features of the building (which should include restricted access, 24/7 surveillance, on-site guards, metal detectors and more) will protect any confidential or proprietary equipment that could potentially exist. Additionally, tracking of assets through serial number capture, scanned bar-codes and sophisticated internal reporting systems will provide you with the ability to understand where your assets are and track these items for internal records.

4. Understand resale channels and confirm ethical methods for reuse.

While data security is priority, some vendors offer solutions for hardware disposition as well. If any equipment still holds resale value, refurbishing and remarketing services can be a great way to maximize your return-on-investment, as well as contributing to the circular economy.

There are a few things that can be done to verify the credibility of a vendor's reuse processes. Steps you can take to evaluate different vendors include:

1. Develop a comprehensive RFP template
   to assist you in your vendor selection. Make sure you ask questions about how they protect your data and how they handle your equipment.
2. Look for third-party certifications and standards
   Common data security standards include include NIST 800-88 r1, HMG IA Standard No. 5 and DIN-66399.Industry certifications include R2v3, ISO 27001, ISO 45001 and ISO 9001.
3. Determine how items are resold
   Trusted sellers on the secondary market will have quality testing and a defined baseline for what is considered sellable, considering age, functionality, appearance and condition. Vendors should have multiple, credible wholesale, distribution and resale channels with good reviews and reputation badges.
4. See the process first-hand
   Go to the site and witness the operation in action. Do the employees appear to have strict standards and protocol? Are the services conducted in a secure environment? Are items handled carefully, and are they cleaned prior to being packaged and resold?

5. Confirm end-of-life assets are shredded and recycled.

If all data has been destroyed and an IT asset no longer holds any resale value, end-of-life disposition is the final step. It is important to ask questions about the final disposition of your end-of-life IT assets because if done irresponsibly your company can suffer grave repercussions. If your equipment ends up illegally dumped, someone can potentially pull the asset tags and determine your company contributed to the toxic environment and wrongful disposition of e-waste.

Responsible recycling vendors provide certificates of destruction and recycling. These documents provide proof that your company chose a reputable company to handle your data and asset disposition program.

As data breaches become more sophisticated there will only be an increasing number of security protocols. The on and off-premises data destruction services provided by SLS provide high-level security services that offer businesses maximum return. These five considerations will help validate your vendor selection and avoid risks tied to data exposure because of IT asset disposition.

Contact us:
www.simslifecycle.com/contact