Compliance Standards, LLC
strategic advisory, research & consulting

66 West Flagler St., 12th Floor, Suite 1204-A, Miami, FL 33130
inquiries@Compliance-Standards.com | Phone: 305-901-6389

More than half of US enterprises don't track their laptops, as 22% of the retired assets are missing

Compliance has been a key requirement driving enterprise IT asset disposition (ITAD), and is indeed a major component of the entire IT asset management domain. Within the broad compliance domain, data security has been, and remains the number one issue of focus in IT asset management circles, including during the phase of IT asset decommissioning. The other major focus that has near top status is cost containment, with environmental stewardship playing a third role in shaping ITAD policies.

The issue of data security is particularly important among the companies that outsource ITAD. In their mind, in addition to the need to handle the physical aspects of moving tens of thousands of decommissioned pieces of electronics and other operational aspects, the ITAD vendors they pick are often selected on the basis that they are perceived to have a solid data security practice. Still, we found that 30% of the companies out there, do not outsource their ITAD function and keep the work internal. Yet, when asked why, they say it's precisely because they don't trust the ITAD vendor on the security front. So regardless of whether companies outsource ITAD or not, data security is front and center in their decisions because they are either facing growing regulatory requirements, and/or due to the ever-expanding data breaches we have come to know and the ones that go unnoticed.

Although most of the incidents of data breach reported by the press tend to be those related to in-network incidents, there is a lot that happens in terms of data breach at the end of life of IT assets. These breaches are generally rarely made public, even though most companies say they do not want to take risks when it comes to discreet and individual assets that are disconnected from their network and moved into the recycling stream.

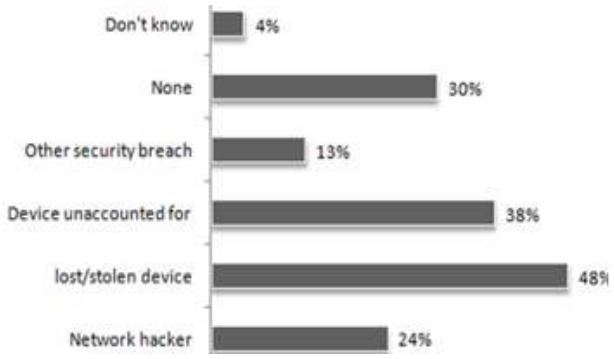
Yet, given the broad economic challenges that companies are facing, the issue of cost continues to weigh considerably on decision-making specific to spending on data security, a problem that is even more severe during the recycling phase due to budget restrictions. These budget limitations often play a key role in perpetuating bad practices at a great risk to the company.

While data security is cited as a priority, practices on the ground challenge this notion and raise questions about the seriousness of the programs designed and implemented by IT departments, and the ability of compliance officers to maintain sanity in the way corporate data is secured.

Dismal State of Data Security: Breaches and Lack of Oversight

Beyond network security, breaches remain alarmingly high at the device level during the useful life of the assets. Such breaches are often the result of a lack of oversight, monitoring and control within the organization and obviously not as a function of outside criminal intent, such as illegal hacking. Indeed, in a survey of 181 large US corporations operating in the financial, healthcare, retail and utility sectors, Compliance Standards LLC found that about one quarter (24%) reported network hacking incidents. The number is large but not shocking considering that there are well organized hackers whose work is precisely to disrupt networks. But when a full 48% of the respondents report lost or stolen devices, this becomes an issue of pure neglect. Almost half of large companies lose their PCs through neglect or theft, highlighting the enormous weak areas of concern, in terms of IT asset oversight. See chart 1.

Chart 1: **Types of Breaches Experienced by US Enteprises**

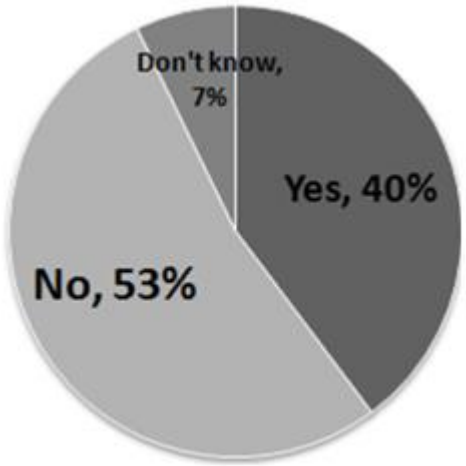


N= 181 US corporations
Source: © Compliance Standards LLC, 2017

In addition, 38% of the companies say they experience missing assets with devices that are unaccounted for. In other words, they don't know if the missing assets were lost by the employee or simply stolen. They just don't have a way of knowing. These figures are exceedingly alarming because they represent higher incidences than the 24% of network hacking. Companies appear to put greater emphasis on network security than on device security, as if the latter carried lesser risk.

It is no surprise then that lost or stolen devices represent a high level of incidence. This is because a majority of 53% of the surveyed companies reported not utilizing any technology to track mobile devices. See chart 2. Only 40% reported to have a way of tracking where their assets are located. With a highly mobile workforce, it is important for companies to adopt the proper tracking technologies that would provide a clear picture of where systems are at any given time. Without such tracking, one should expect that data can be lost.

Chart 2: **US Enteprises' Tracking Laptops**



N= 181 US corporations
Source: © Compliance Standards LLC, 2017

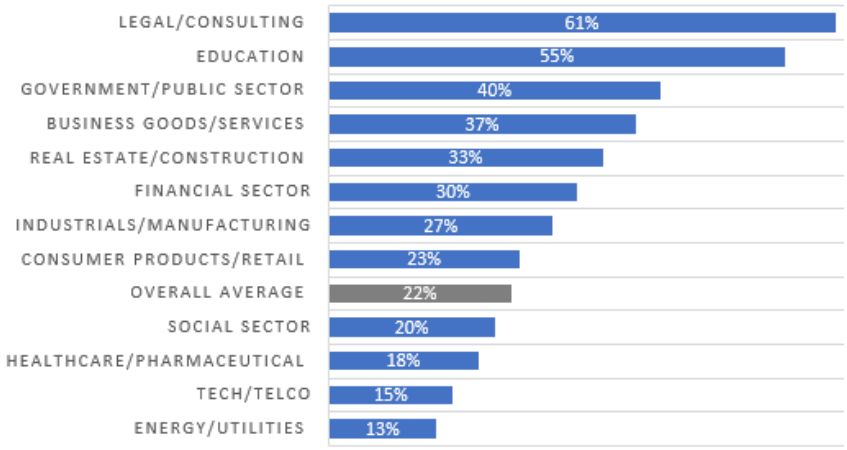
IT Asset Disposition: The Other Weak Link

The IT asset disposition sector (ITAD) has gathered greater attention over the last decade, amid rising interest in Green IT. Although it has always been an orphaned function due to several factors, including budgetary neglect, ITAD is critical because millions of data-bearing assets move into the

secondary market each year with data still on them. Reputable ITAD vendors tend to do the right things to ensure that their clients' data are wiped. But it is often the case that the original owners of the assets seem less concerned and allow the devices to move without proper security procedures.

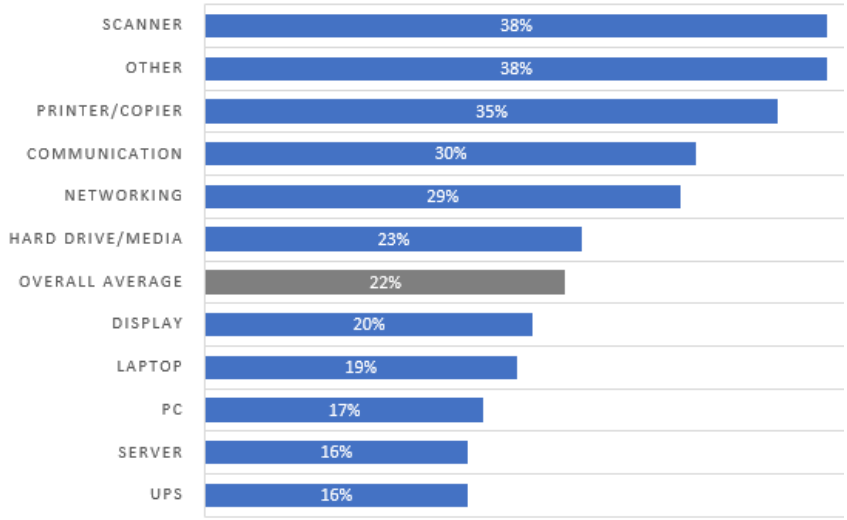
In general, asset manager should perform several asset reconciliation tasks to ensure that what they retire ends up tracked and data-wiped appropriately. Most individuals would assume that it is at the ITAD vendor's facility or during the transportation phase that assets are lost. The reality is rather shocking. More frequently, losses actual happens at the user side before an ITAD vendor is engaged. In fact, only 78% of assets retired by companies are successfully tracked to a disposal vendor, meaning that 22% of the inventoried assets retired by companies are nowhere to be found or cannot be matched by serial number.

Chart 3: **% of mising retired IT assets through serial number matching**



N= more than 400K devices analyzed
Source: © Retire-IT & Compliance Standards LLC, 2017

Chart 4: **% of missing retired IT assets, by asset type, through serial number matching**



N= more than 400K devices analyzed
Source: © Retire-IT & Compliance Standards LLC, 2017

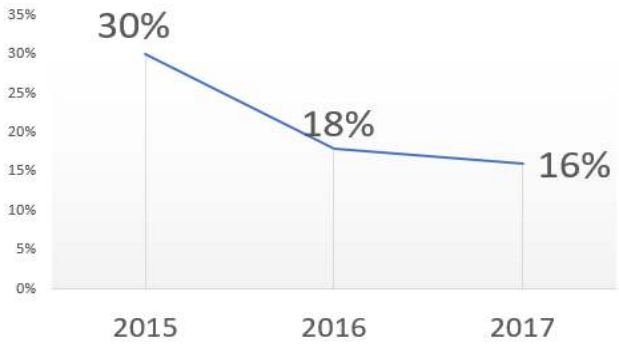
Although the figure is shocking, it does confirm the results of the survey cited earlier. While data suggests that serial number matching has improved over the past couple years, perhaps as an indication that companies are taking their responsibility more seriously and putting forth greater effort to provide accurate inventory, the risks related to the still missing assets far outweigh the gains companies have made in terms of tracking. Still, companies may be ignoring the larger issue by not looking at tracking data. During ITAD, a common approach is for companies to allocate retired assets to an ITAD vendor rather than track. Allocating inventory effectively conceals losses because it assumes assets are received by the ITAD vendor, thus disregarding important issues such as employee theft.

The data analyzed by Compliance Standards was provided by ITAD services company Retire-IT. The company offers disposal tag chain-of-custody tracking services, essentially interfacing between the end-user company and its ITAD service

provider as a way to inject third-party reconciliation and auditing functions. This analysis utilized a random sample of 4,812 ITAD projects, combining a total asset volume of 402,363 units, across 732 companies. As such, the data is not only extremely relevant to the debate, but also very accurate given the direct access to hundreds of thousands of assets analyzed.

The data independently analyzed by Compliance Standards indicates that when ITAD vendors take possession of assets leaving their customers, 22% of the assets that the end-user expects to retire are unaccounted for when tracked by serial number. The weakness is not from the ITAD vendor, but from the inherent weakness of the tracking systems. When tracked by barcoded disposal tag, 98.4% of assets are track. Asset managers have long recognized benefits of barcoding IT assets at procurement. Applying barcoded disposal tags during IT asset disposition may be even more beneficial, especially from a security and risk management perspective. Disposal tags are considerably more effective for tracking than serial numbers, and they have the added benefit of deterring employee theft.

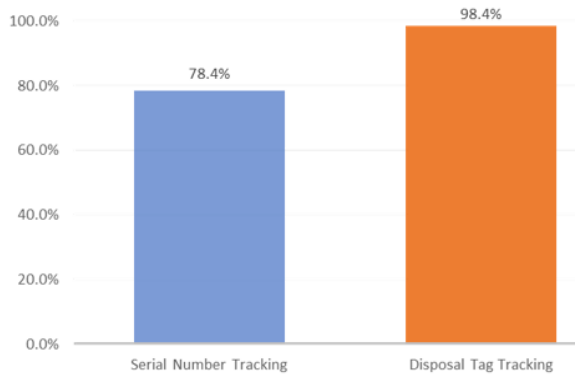
Chart 5: **Serial Number Tracking. Rates of missing devices per year**



Source: © Retire-IT & Compliance Standards LLC, 2017

The results vary dramatically by industry. Energy, Technology, Healthcare, and surprisingly the Social sector, such as charities and associations were most successful. Ironically, government, education, and law firms, three types of institutions trusted to keep public data secured, did worst. Likewise, financial firms performed below average.

Chart 6: **Serial Number vs. Disposal Tag Tracking Success Rates**



Source: © Retire-IT & Compliance Standards LLC, 2017

Tracking by device type varies dramatically, too. Fortunately, data bearing devices are tracked more successfully than other types of equipment. However, almost any type of asset has the potential to store or access data, so companies should be careful. With the evolution of Internet-of-all-things (IoT), the challenge is likely to grow exponentially over in the foreseeable future.

It is clear that many organizations do not take tracking seriously, when it is evident that the tracking function allows verification and can be utilized during litigation or similar situation. Organizations with mature security procedures might naively assume they are protected because they have a policy that requires drives to be encrypted or physically removed/destroyed. But lack of tracking makes any such stance irrelevant, if one has no idea where the asset is.

Companies have a regulatory requirement to perform a risk assessment when a loss occurs. The loss of an asset should trigger an incident report which in turn requires a risk assessment. Documentation must exist to demonstrate that there is no potential data breach. But if the asset is missing, and unaccounted for, the risk now becomes substantially higher.

Reasons behind the weakness:

Specific to the ITAD function, the lack of due diligence in the enterprise is largely organizational. The vast majority of companies report that the ITAD function is essentially handled by their IT department. Unfortunately, IT departments are ill prepared to deal with the requirement of a compliant ITAD. IT department staffs are well suited for functions that span from asset deployment, to day-to-day tasks of managing those assets, such as software upgrades and patches, to physical repair of assets. IT staffs work well with their procurement and sourcing colleagues in drafting asset requirements from a brand new hardware and software perspective. But when it comes to end-of-life management, there is a major functional disconnect. ITAD requires several areas of oversight that are not part of IT staff's skill set. Data security and environmental stewardship are often the domain of professionals from legal, compliance, sustainability and corporate social responsibility. Financial considerations and cost containment require a good dose of accounting and financial knowledge. There is the need to understand more than the basics of the secondary market. There are issues related to facilities management, and many other tasks. In this context, asking IT staffs to perform these tasks in addition to their obligations is a major disconnect that is a clear source of risk. As long as these organizational functions are not overhauled and properly aligned, the data security risk will remain permanent.

About Compliance Standards LLC

Compliance Standards LLC is a premium advisory, consulting and research service that provides management and market intelligence specific to IT management, IT asset life cycle, all the way to electronics products end of life. Our coverage focuses not only on compliance issues, but also on discovering best practice, efficiencies, cost control techniques and brand protection.

Compliance Standards provides proprietary engagements, research and consulting to customers on both the supply side (vendors and service providers) and demand side (end-users), as well as commentary, expert analysis and published discussions on the topic. In addition to our premium advisory and research services, we are building an industry network within our site comprising of members of ITAM ecosystem.

To find out about our services and solutions, please visit: http://bit.ly/2wMOFbU

Compliance Standards Analysts are located in Miami, Boston and Las Vegas. Our mailing address is in Miami, at:
66 West Flagler Street
12th Floor, Suite 1204-A
Miami, FL 33130, USA
Phone: 508-981-6937

Disclaimer and Copyright Notice

The information contained herein has been obtained from primary research and sources believed to be reliable. Compliance Standards LLC disclaims all warranties as to the accuracy, completeness or adequacy of such information. Compliance Standards LLC shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

inquiries@Compliance-Standards.com
Phone: 508-981-6937