Morgan Stanley was recently fined $60 million “for engaging in unsafe or unsound practices relating to information security and noncompliance with 12 C.F.R. Part 30.” The findings of the Office of the Comptroller of the Currency (OCC) included that Morgan Stanley failed to maintain proper inventory of devices that contained customer data. Furthermore, the bank failed to assess the risks of using third-party vendors and do proper due diligence on those subcontractors.

Frankly, it was only a matter of time before something like this happened to a major enterprise organization. When I spoke at the E-Scrap Conference two years ago, I stated that it was only a matter of time before an ITAD company was involved in a data breach. While we still don’t know who the responsible ITAD vendor was, or how exactly they failed to protect Morgan Stanley, there are two key places where their processes could have broken down and resulted in a data breach.

The first problem area is with the data destruction process itself. When I first entered into this industry data security was what kept me up at night. The idea that a hard drive would be resold without being wiped was a real threat. I often compared it to gun safety. Always assume a gun is loaded or a hard drive has data, and always double- or triple-check. Utilizing separate employees, third party random forensic audits, and other mitigation factors lets me rest easy knowing my clients are protected.

The second problem area is documentation. At a typical CyberCrunch training session employees hear me say… “data destruction is only half the process the other half is the documentation. The documentation is just as important as the actual destruction.” I find that keeping records can be more difficult than the actual destruction and testing process. Without adequate records, it's like the process never occurred. The Morgan Stanley incident further affirmed my fears that many ITAD companies do not follow through on their documentation process. Unfortunately, delayed, incomplete or missing documentation is all too common in the industry.

How can companies mitigate these risks? Proper paperwork and reporting are expensive -- but so are the fines and lawsuits that come with a data breach. It’s a labor-intensive process to capture serial numbers of equipment, especially non-working equipment. We see multi-billion dollar companies who decline asset reporting because it costs a few hundred dollars. With IT budgets declining, CFOs and CTOs need to ensure that end-of-life asset management is factored into the total cost of ownership.

What does the future hold? My biggest concern industry wide is the lack of knowledge about solid state drives (SSDs). These require special wiping software and hardware. Many companies, ITAD providers and third-party regulators do not understand how SSDs store data and how they need to be wiped and/or destroyed. I see companies drilling through SSDs and completely missing the circuit board, or using outdated wiping processes that are not approved for SSDs. Or devices with M.2 SSDs on the motherboard that the vendor doesn’t recognize as a storage device.

Every organization should require detailed paperwork from their ITAD vendor. Document your due diligence process. Visit their site. Ask questions about their process. Demand complete and on-time paperwork. If an ITAD vendor can’t provide adequate answers or sufficient documentation, find one who can.

While risks of end of life asset disposition cannot be eliminated, it can be drastically reduced by using proper tools, processes, and following up with good documentation.

About CyberCrunch

CyberCrunch provides data destruction, IT asset disposition, and electronics recycling services to businesses, organizations, and government agencies. CyberCrunch specializes in helping businesses to comply with government and industry regulations like HIPAA, PCI-DSS, GLBA and SOX. CyberCrunch provides its services to customers nationwide from its headquarters in Greensburg, PA and its facility in Aston, PA.

Contact

https://www.ccrcyber.com/contact/

info@ccrcyber.com

(866) 925-2354