ADISA

SEPTEMBER 2012 ISSUE 2

IT ASSET DISPOSAL • RISK MANAGEMENT • COMPLIANCE • IT SECURITY • DATA PROTECTION

FEATURE: Exploring the links between cybercrime and e-waste

Pages 5 and 15

GHOSTS FROM THE MACHINES: 10 years of discarded data

Page 19

Images Supplied Courtesy of Davison/Greenpeace

The US ITAD market space

by Kyle Marks, CEO of Retire-IT

Kyle Marks, CEO of Retire-IT

The ITAD industry in the US has matured rapidly in the past few years. Media coverage has increased public awareness of the environmental problems and privacy concerns when discarded equipment is discovered in third world countries, or when confidential data falls into the wrong hands.

Environmental concerns have pushed roughly half the States and several cities to pass environmental legislation. On top of numerous Federal data security laws, a large majority of States have also enacted breach notification laws of their own. HIPAA (Health Insurance Portability and Accountability Act) receives the majority of media attention, but more than 500 various laws now affect ITAD.

Today, all leading ITAD vendors elect to become "certified" to a voluntary environmental standard, either e-Steward and/or R2. Also, every ITAD vendor claims adherence to stringent data security standards (DOD or NIST). A small but growing number of ITAD vendors have elected to become NAID certified to bolster security credentials.

While the industry has standardised and services have evolved, advances with American corporate end-users have not kept pace. Employee theft is the biggest threat to ITAD. Internal ITAD activities are often performed by low-level employees who are given little or no guidance from senior management. Few organisations have formal ITAD policies. Even fewer have formal controls in place. It is no surprise when off-network devices turn up missing.

Data security laws mandate that organisations implement "adequate safeguards" to ensure privacy protection of individuals. Organisations do a fair job of protecting systems in-use, but they fail miserably when it comes to protecting data residing on retired equipment. They are beginning to pay the price when there is a breach. Violators face increased pressure from Federal and State authorities. In addition, they incur heavy remediation costs and are being forced to defend against expensive privacy class action lawsuits.

This year, the Office of Civil Rights (OCR) began to apply unprecedented sanctions for HIPAA security violations against private companies and public agencies. In May, the OCR fined BlueCross BlueShield of Tennessee (BCBST) $1.5 million for violations following the theft of 57 unencrypted hard drives in 2009. In June, the OCR also fined Alaska's Department of Health and Social Services $1.7 million following the theft of a USB hard drive in 2009.

Significant fines following breaches may become the norm. The OCR stressed that organisations must "have in place meaningful access controls to safeguard hardware and portable devices." They "expect organisations to comply with their obligations under these rules regardless of whether they are private or public entities."

Federal agencies are not the only ones eager to punish violators. Last May, the Massachusetts Attorney General fined Boston's South Shore Hospital $750,000 following the loss of unencrypted computer tapes in 2010. The tapes were sent to a disposal vendor to be erased and recycled. But the hospital did not determine whether the disposal vendor actually had sufficient safeguards in place to protect sensitive information, among other issues.

There is no doubt that State and Federal penalties can be punitive and painful. However, the effect of a privacy class action lawsuit can be much worse. Following the loss of a backup data tape in 2011, healthcare benefits provider TRICARE was hit with eight separate privacy lawsuits, including one seeking $4.9 billion in damages. The suits allege that TRICARE and its subcontractor were negligent. TRICARE has been accused of "intentional, willful and reckless disregard of Plaintiffs' privacy," and for failing to respond to "recurring, systemic, and fundamental deficiencies in its information security."

Historically, privacy class actions falter for inability to prove recoverable damages, but this probably provides little consolation. The cost of defending privacy suits can cost millions. And, let's not forget remediation costs. In the case of BCBST, the cost of the fine was just the tip of the iceberg. In addition to the penalty, BCBST reportedly spent $17 million in investigation, notification and protection efforts.

Whether or not you are involved with the US healthcare industry, these cases draw attention to basic elements of an effective information security, especially the need for adequate safeguards pertaining to off-network and retired devices. When evaluating sufficiency of their ITAD policies and procedures, organisations must be mindful of potential administrative fines, remediation expenses, and the possibility of costly privacy class action litigation.

About the author:
Kyle is the Founder and CEO of Retire-IT. Prior to founding Retire-IT, Kyle was an executive with RetroBox, a leading IT asset disposal company that is now Arrow-Intechra. Previously, Kyle was an executive with WEGO Systems, a consultant with Bain & Company, and held numerous marketing positions with Maybelline. Kyle has a Bachelor of Arts in Economics and Business Administration from Rhodes College, and a Masters in Business Administration from Harvard Business School.

Kyle is also an IAITAM CHAMP (Certified Hardware Asset Manager Professional of the International Association of Information Technology Asset Managers).