Consider ITAD a Security Incident

A Practical Look at ITAD Security Issues

By: **Kyle Marks, CHAMP**
CEO, ***Retire-IT, LLC***

Organizations that focus on privacy take a serious look at all areas of potential vulnerability. One area of unappreciated vulnerability is the process of IT asset disposition (ITAD). When evaluating the sufficiency of any ITAD policy, organizations must be mindful of possible administrative fines, expensive remediation outlays, and costly punitive class action litigation. To ensure adequate safeguards are in place, IT asset managers should consider treating ITAD as if it were an inevitable security incident.

Breach Versus Incident

A data security incident is a situation that results in protected data potentially being viewed, used, or stolen by an unauthorized individual. When an incident occurs, a subsequent investigation is undertaken to determine whether or not there was a breach. The investigation determines if there was or was not a release of protected information to an untrusted environment.

Several factors determine if a release qualifies as a breach, including the number of individuals affected. It is important to recognize that a breach is a breach, regardless if data is accessed, regardless if individuals suffer actual damages, and regardless if there is public disclosure (more on this below).

Of course, not all security incidents rise to the level of breach. However, compliance requires all data security incidents be investigated.

Incident Response

When a data security incident occurs, an obligation is created to prove there was not a breach. The burden of proof belongs to the organization. Incident response plans are designed in advance to reduce risk and ensure the burden of proof can be met.

Mature organizations approach security incidents in a systematic way. Established standards, procedures, and guidelines must be followed to ensure a consistent and timely response. Besides being more efficient, a methodical incident response has the added benefits of reducing real damages if a breach occurred.

Response procedures vary depending on the type and severity of security incident, but each has pre-defined steps (e.g. discovery, documentation, notification, containment, investigation, resolution, etc.). For each step, there are activities prescribed. For example, investigations typically include evidence collection, retention, analysis, and prioritization.

ITAD is an Incident

Organizations handle ITAD in different ways. Most commonly, retired IT assets are transported to a certified electronics recycler to be properly processed and sanitized. When a data-bearing asset is shipped to a disposal vendor, there is a real possibility that asset could be lost or stolen in-transit. Because of the potential for release of protected information to an untrusted environment, it is wise to consider every disposal shipment as a security incident waiting to happen.

Many organizations have already recognized the risk of in-transit loss. An increasing number of organizations now destroy data in-house, prior to disposal. The logic follows that if data is destroyed before a move, any loss of a particular asset might be unfortunate, but not be a disaster. In other

words, the loss of an already sanitized asset might be considered an incident, but would not result in a breach.

While in-house data destruction is part of an effective disposal strategy, it is not sufficient. A policy of pulling and/or wiping hard drives from computers before disposal can create a false sense of security. Overly confident organizations often overlook other vulnerabilities. The biggest threat to ITAD occurs before a disposal project begins. Trusted insiders can take retired assets before data is destroyed.

Securing or destroying data before a move is wise. However, if an asset is lost or stolen in transit, there still must be convincing evidence for that specific asset showing it could not contain recoverable data. Someone saying that they wiped a hard drive is considered hearsay. When data is destroyed, there must be unimpeachable evidence.

Investigating ITAD Incidents

Envisioning each ITAD project as an inevitable security incident is a valuable exercise - one that can help IT asset management establish adequate safeguards and controls to inhibit an incident from becoming a breach. ITAD incidents occur at three different points; before an asset is shipped, during transit, and at the disposal vendor. For this exercise, we consider only in-transit and disposal vendor-related incidents, and focus simply on hard drives.

In order to resolve any ITAD security incident, IT asset managers require two types of evidence:

A. Chain-of-custody
B. Data destruction

If an asset is received by a qualified disposal vendor, it is reasonable to assume there was no release of private information during transit. If data destruction evidence exists, it is reasonable to conclude no breach occurred. Anyone who has managed an ITAD project will attest that obtaining unimpeachable evidence for chain-of-custody or data destruction is easier said than done.

Chain-of-custody is proven by tracking assets. Data destruction is proven by obtaining evidence that the hard drive(s) in a particular asset was sanitized or physically destroyed.

Detailed inventory reconciliation is required to determine if any particular asset is missing. If no evidence exists to prove that an asset was received (by the disposal vendor), that asset must be presumed lost or stolen. Efforts should be taken to locate the missing asset. If the asset cannot be located, having evidence of data destruction becomes essential.

Whether data destruction is done in-house or off-site, IT asset managers should obtain and retain proof. For a hard drive purported to be wiped, this requires a tamper-proof log file detailing successful software overwrite corresponding to the asset. For a hard drive purported to be physically destroyed, this requires a serialized inventory detailing the date of destruction, method of destruction, and person responsible, corresponding to the asset.

Independent Verification

Evidence of chain-of-custody and data destruction must be reliable, verifiable, and unimpeachable. Therefore, verification cannot be outsourced to the disposal vendor or delegated to the same employee responsible for physically performing ITAD activities.

Security incidents go undetected when an organization relies on employees to self-report incidents. Naturally, employees tend to report self-serving interpretations of the facts, especially when facts could make them look bad. Without independent reporting and verification, management receives heavily distorted information about incidents (if any).

A critical aspect of every major data security law is that organizations must minimize segregation-of-duties conflicts that create opportunities for theft and fraud. The focus to-date has been on access privileges (for example, if an employee has the ability view private information without authorization). Considering ITAD an inevitable security incident gives IT asset management the objectivity necessary to see inherent conflicts-of-interest exist with ITAD programs as well.

ITAD is Inevitable

The theft or hack of an asset can result in headline-grabbing news. When an IT asset is being used by an organization, it is susceptible to all sorts of technical and physical attacks. Thankfully, not every asset is the target of an attack. During its lifecycle, an asset may never be attacked. Disposal is different. Unlike an attack, ITAD is inevitable.

The frequency and size of newsworthy breaches resulting from sophisticated attacks seems to be increasing. It is no surprise that organizations spend billions of dollars each year to thwart attacks. Organizations expend comparatively little to safeguard against ITAD incidents.

I am not suggesting that organizations reduce efforts to protect assets when they are being used. I am suggesting they

allocate adequate resources for IT asset managers to protect assets when they are retired.

Legal Obligations

Privacy laws mandate that an organization put in place adequate safeguards and effective controls to prevent and detect data security incidents. They also mandate that an organization must disclose any breach.

If a tree falls in a forest and no one is around to hear it, does it make a sound? Privacy advocates probably don't care. If a breach occurs and no one is around to hear about it, it is still a breach and privacy advocates do care. Disclosure provisions in privacy laws exist because organizations will not voluntarily advertise costly and embarrassing breaches.

An organization faces more serious sanctions and likely punitive litigation if it disregards the disclosure obligation and a breach is later discovered. Considering ITAD an inevitable security incident will elevate the importance of IT asset management's role in preventing potential data breach.

In Conclusion

In the movie The Matrix, Morpheus offed Neo the option of taking the blue pill or red pill. IT asset managers already know about the painful truth of reality regarding ITAD data security risks. We don't get the choice of blissful ignorance. Even

though organizations seldom view ITAD as an **inevitable** security incident, IT asset management should.

Acknowledging risks and inherent conflicts-of-interest will result in more effective ITAD policies and adequate safeguards. Applying established incident response procedures to the unavoidable process of ITAD can help raise awareness of unappreciated vulnerabilities.

Educating senior management about the risks will hopefully secure IT asset managers the resources needed to prevent an ITAD-related breach. Neo never knew about the Matrix until Morpheus opened his eyes. IT asset managers should consider ITAD an inevitable security incident, even if others do not yet recognized it as such. Management may still decide to swallow the blue pill, but we should give them the choice.