5 Security Holes You May Have Missed In Your Hard Drive Retirement Process

Introduction

Retiring hard drives and other storage hardware is a necessary but often neglected part of every corporate data security plan. However, many companies gloss over this process and leave potential holes that can be exploited. Fortunately, these holes are easy to fix with a little awareness and the right tools. This whitepaper explores 5 commonly missed security holes when retiring hard drives and ways to fix them.

5 Security Holes

1. INADEQUATE REPORTING

Secure and comprehensive reporting should be a central part of your hard drive retirement plan. Without proper reporting, you remain potentially liable for data breaches. To properly protect your company you need bullet-proof, auditable reports.

Physically destroying hard drives is particularly weak when it comes to reporting. Physical destruction records can often be faked, altered, or prone to human error.

Free software wiping tools also are problematic because they don't have robust, auditable reporting. You can't store reports in a corporate database or import report data into third-party tracking tools.

Fortunately there are software wiping tools that will securely and permanently erase all hard drive data while providing bullet-proof reports as we'll discuss later in this whitepaper.

2. REMOTE LOCATION RISK

Retiring computer hardware in your corporate headquarters is a relatively simple, straight forward process. Your in-house IT staff can securely transport them and remove any sensitive data. However, when dealing with remote locations you lose much of this control. Remote locations may not have a dedicated IT staff or the tools to wipe your hardware onsite. Transporting computers back to your headquarters is an option, but at a very high cost and not without its own risk; there's often no way to monitor what happens to a computer between the time it's decommissioned and the time it's actually shipped back to HQ. Employees or others at

the remote location may still be able to access data on the computer during the interim time period. In addition, transporting computer hardware using a secure chain of custody can be very costly and even prone to its own security holes.

3. WEAK INTERNAL CHAIN OF CUSTODY

Internal risk occurs if your chain of custody process is either inherently flawed or not enforced diligently. Examples of flawed processes include not collecting hardware promptly after it's decommissioned or having a high touch count (too many people accessing or handling hardware). Examples of processes that are not diligently enforced include leaving computer hardware in unsecure locations or allowing unmonitored access, intentionally or unintentionally, to decommissioned computers.

4. WEAK EXTERNAL PROCESSES (OUTSOURCING RISK)

External risk occurs when using a third party provider to handle data destruction. Many organizations don't realize that when using a third party provider for data destruction their secure data and hardware is being handled in many cases by transient or temporary employees. While these providers may offer a "secure" chain of custody, you are still relying upon the integrity of the employees themselves and making the assumption they are properly trained and trustworthy.

5. RELYING SOLELY ON ENCRYPTION

One emerging trend is for hard drive manufacturers to make drives encrypted as a native feature. The value proposition is that if you need to retire or recycle the drive, you simply delete the encryption key and your data is safe. While it may be true that the data isn't accessible in a practical sense, it's still on the drive and still presents a risk in the longer term. Encryption technologies are constantly changing and improving as are the tools to break encryption. The encryption technologies from 10 or even 5 years ago are relatively easy and even routine to crack today. So while relying on a deleted encryption key to protect your data today, you may face the risk that it will be simple to crack in the future making you still vulnerable to liability. Add to this that services like Amazon's computing cloud making large-scale computing power easily available to your average person, including hackers and those with ill intent, providing additional firepower for those attempting to crack encryption keys.

Another problem with relying solely upon encryption is that hackers attempting a brute force crack may get lucky and stumble upon the correct encryption key with less than the typical effort.

How To Fix Your Security Holes

There are several steps you can take to ensure your hard drive retirement processes are secure. The following suggestions will help you solve the 5 holes mentioned above and tighten your security policy regarding retired drives.

ENSURE REDUNDANCY IN YOUR PROCESSES

Part of the key to high security when destroying your data is redundancy. One way to provide redundancy is to have multiple methods of data destruction. Most commonly large corporations and government organizations will often wipe the data with a software tool and then physically destroy the drive.

When using two forms of data destruction implement the method that is fastest and most reliable first. This is typically a software wipe since it can be deployed quickly and remotely.

Once a hard drive is wiped, it can then be transported or handled with much less risk. By using a certified software tool, you should have no risk of compromised data from that point on. Then, you can physically destroy the drive or transport it to a recycler to recover recyclable precious metals and handle the hardware in an environmentally friendly way.

Another way to introduce redundancy is to audit your process which is mentioned later in this whitepaper. Having comprehensive and secure reporting is vital to accurately auditing your processes.

DECREASE THE NUMBER OF CRITICAL "TOUCH POINTS"

Your risk naturally increases with the number of people who touch, access, transport, or handle a hard drive. A critical touch point occurs when an employee handles or accesses a decommissioned computer while data is still accessible on the hard drive. Once data is erased from the drive, additional touch points don't increase risk, just cost.

Using the proper hard-drive wiping tools, you should be able to decrease the number of critical touch points to 1-2 maximum. Most all computers can be wiped by an IT staff member either in person or remotely using capable wiping software.

DECREASE PERIOD BETWEEN DECOMMISSIONING AND PROCESSING

A computer should ideally be erased and processed the same day it is decommissioned. Otherwise you run the risk of unauthorized personnel accessing the computer and compromising sensitive data. Remote software wiping or in-person on-site wiping are the most

efficient, cost-effective, and fast ways of initially processing a computer. These methods can be deployed quickly and can be 100% effective in removing data giving you assurance the computer is secure even if it can't be immediately transported or processed further.

ESTABLISH A SECURE PROCESSING LOCATION

Once computers or hard drives are decommissioned, it's important to store them in a secure location, particularly if the data hasn't been removed. Some companies dedicate a secure room to perform largescale PXE software wipes. It's important that the room can only be accessed by authorized personnel.

USE SOFTWARE WIPING WITH SECURE REPORTING

Hard drive wiping using properly-certified software is the most effective form of data destruction available today. With the proper certified software data has been shown to be impossible to recover even by the NSA (you can see an example of the WipeDrive certification at http://www.niap-ccevs.org/st/vid10395/). One significant benefit software wiping has over physical destruction is the ability to generate audit logs. These logs are verifiable, impossible to manipulate, auditable, and immune to human error. This level of proof provides valuable protection against legal action and peace of mind for company owners and shareholders who want to ensure proper security measures are taken.

FULLY VET OUTSOURCED PROVIDERS

When using outsourced providers of data destruction, be sure to ask specific questions about their process to ensure they are using best practices. Here are a few key questions to ask:

1) Who physically handles the hardware and how are they trained? You ideally want trained and licensed technicians rather than low-cost temporary labor. As a follow up, ask what licenses or certifications they have.

2) Are your destruction reports fool-proof? Can they be inaccurate due to manipulation or human error? Some outsourcing companies may have special processes to help ensure the reports are accurate and secure.

3) How many people have physical access to the drive before it is destroyed? This should be as low as possible and ideally only one person.

4) What methods of data destruction do they use? Physical destruction is generally more costly and less secure. Software destruction is preferred, but only if they are using certified tools. NIAP-certified software is ideal.

AUDIT YOUR INTERNAL PROCESSES

Assign an objective or outside party to audit your current procedures for processing decommissioned computers and hard drives. Measure how long it takes for a computer to be processed once it's decommissioned. Observe where and how long computers are accessible by other employees after being decommissioned. What measures are taken to process the computer? Is the processing area secure and accessible only by authorized employees? Are processes kept and followed accurately or loosely? Audits usually reveal many insightful results and can serve as an effective and convincing way to upgrade your policies or ensure they are followed more closely.

Conclusion

By taking a few easy steps and by using the right tools you can address many of the common holes in your hard drive retirement process. With mobile technologies and small high-capacity mobile storage, data is easier than ever to capture and transport. Accordingly, organizations need to be vigilant and aggressive in how they deal with decommissioned computers and recycled storage hardware. By following the suggestion above, the goal of closing your security holes is possible.