7 Security Gaps

You May Have Missed In Your Drive Retirement & Disposal Process

www.ducorestealth.nl | info@ducorestealth.nl | +31 (0) 320 809985

Introduction

Disposal of drives and other data-bearing hardware is a necessary but often neglected part of every organization's IT lifecycle. However, many companies skim over this process and leave potential gaps that can be exploited. Fortunately, these gaps are easy to fix with a little awareness and the right tools. This whitepaper explores seven commonly missed security gaps when retiring their drives and resolutions.

1. INADEQUATE REPORTING

Secure and comprehensive reporting should be a central part of your IT asset disposal plan. Without proper reporting, you remain potentially liable for data breaches. To properly protect your organization you need certified, auditable reports.

Physically destroying drives is particularly weak when it comes to reporting. These reports comprise of a technician's ratification that they saw the drives be destroyed. Physical destruction records can often be faked, altered, or are prone to human error.

Free software and OEM wiping tools also are problematic because they don't provide robust, auditable reporting. These tools also lack the capability to store reports in a corporate database or export report data into third-party ERP systems.

IT asset wiping using properly certified software (like WipeDrive) is the most effective form of data destruction available today. With a certified erasure software, data has been shown to be impossible to recover. 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. Certified tools also integrate their reports into ERP and 3rd party systems.

2. REMOTE LOCATION RISK

Disposing of computer hardware in your corporate headquarters is a relatively simple, straight forward process. Your in-house IT staff can securely transport the IT assets 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 arrives at headquarters. Employees or others at the remote location may still be able to access data on the system 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 gaps.

We recommend that a computer 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. Providing assurance that the computer is secure even if it can't be immediately transported or processed further.

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.

A recommendation to fill this gap would be to have all systems erased immediately before leaving their initial location. 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 drive wiping tools, you should be able to decrease the number of critical touch points to 1-2 maximum. Most computers can be wiped by an IT staff member either in person or remotely using capable wiping software.

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 assuming the technicians are properly trained and trustworthy.

This gap could be filled by a NAID/eStewards certified organization to handle your IT systems.

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 is used? 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.

5. RELYING SOLELY ON ENCRYPTION

Most drives are 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 easily accessible, the data is still on the drive and presents a risk in the

long term. Encryption technologies are constantly improving but so are tools used 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.

Encryption keys can also be broken by a brute force attack that may be able to unlock your system. The removal of the encryption key will allow all the data on the drive to be accessed. It is our recommendation to securely erase drives with bit by bit or chip-based erasure patterns to ensure all data is unrecoverable, regardless of the encryption on the computer.

6. UNKNOWN PROCESSES FOR DATA SECURITY POLICY

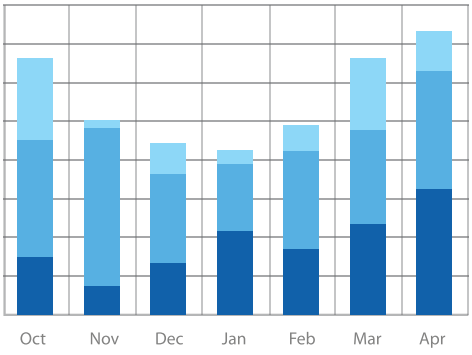
Organizations lacking a data security policy and the processes within the data security policy open themselves up to security gaps. If processes are left to the technician to develop and follow, they may not fully cover the gaps in your data protection policy. Processes should be designed by the management team and team members trained on the components of that process.

We recommend reviewing your data security policy and creating processes before IT assets need to be disposed of. This can limit your exposure to data breach possibilities and provide clarity to all team members on the steps involved.

7. FAILURE TO AUDIT INTERNAL PROCESSES

An important part of any data security policy is to have a 3rd party audit your procedures for processing decommissioned computers and drives. The audit should measure how long it takes for a computer to be processed, observe where and how long computers are accessible by other employees after being decommissioned and report on what measures are taken to process the computer. The audit should check that the processing area is secure and accessible only by authorized employees, and many other components.

Audits usually reveal many insightful results and can serve as an effective way to upgrade your policies or ensure they are followed more closely.



How To Fix Your Security Gaps

There are several steps you can take to ensure your drive retirement and disposal processes are secure. The following suggestions will help you solve the 7 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 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 data breaches 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.

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 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 & PROCESSING

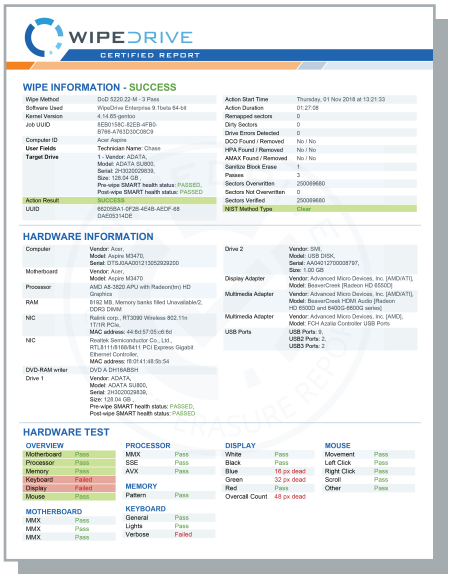
A computer should ideally be erased and processed the same day it is decommissioned. Otherwise you run the risk of unauthorized personnel accessing the computer and compromising sensitive data. Remote software wiping or in-person on-site wiping are the most efficient, cost-effective, and fast ways of 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 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 large scale PXE software wipes. It's important that the room can only be accessed by authorized personnel.

USE SOFTWARE WIPING WITH SECURE REPORTING

Drive wiping using properly-certified software is the most effective form of data destruction available today. With the proper certified erasure software data has been shown to be impossible to recover. 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.


WIPEDRIVE
CERTIFIED REPORT

WIPE INFORMATION - SUCCESS

HARDWARE INFORMATION

HARDWARE TEST

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. Know who and how many people physically handles your assets before they are processed. Be sure you are comfortable with their data destruction methods and be sure to obtain tamper-proof destruction reports.

AUDIT YOUR INTERNAL PROCESSES

Assign an objective or outside party to audit your current procedures for processing decommissioned computers and 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 gaps in your IT asset disposal 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 suggestions above, the goal of closing your security gaps is possible.