DECOMMISSIONING IT:

ENSURING DATA SECURITY AND BRAND PROTECTION

CentricsIT

WE SEE IT DIFFERENTLY

CONTENTS

THE IMPORTANCE OF PROPER DECOM

“It takes 20 years to build a reputation, and five minutes to ruin it.” —Warren Buffett

No one wants to be the next big data breach. And because data is one of your company’s most valuable assets, you must guard it by whatever means necessary.

It’s why you have physical security both in and outside of your data centers. It’s why you establish keyed encryption to prevent unauthorized root level access to your servers. It’s why you keep strict maintenance schedules to ensure that all software is upgraded and patched. It’s also why you conduct annual cybersecurity training sessions for your employees and require them to change their passwords on a regular basis.

You jump through a series of digital and physical hoops, knowing that each measure is necessary for the end goal—to protect your assets and to stay out of the news. So, you establish and follow meticulous protocols and best practices to keep your data as secure as possible.

At least, while you’re using it.

END-TO-END RESPONSIBILITY

What happens when you start decommissioning units and recycling EOL hardware?

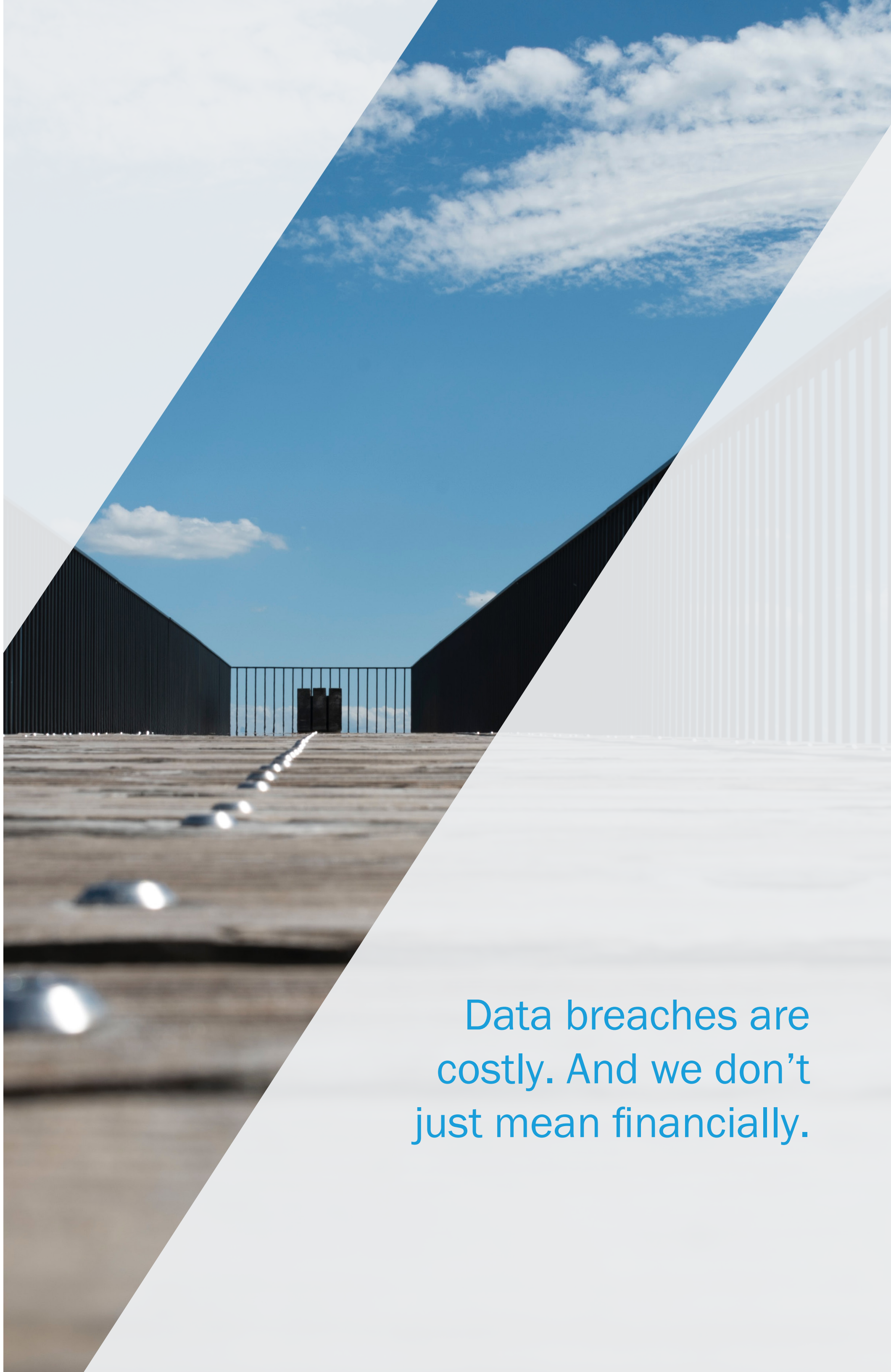
You already spend a great deal of time, money, and human resources defending your active data. Why let that work and investment go to waste by failing to administer the same security diligence for data after its hosting hardware has been phased out of your facilities? You may no longer need those units, but that doesn’t mean your data security responsibilities end there. Rather, you should secure the residual data with the same dedication with which you safeguard your active hardware and data (because we all know how ugly data breaches can be).

THE LATENT RISK OF DISCARDED DATA

As we have seen in the past with companies like Target, Yahoo, and Equifax, data breaches caused by human error or negligence can impact the financial success and popularity of your brand for years to come.

Consider the following:
The Target data breach began when cybercriminals stole network credentials from a third-party HVAC vendor[1] and used them to hack into the retail giant's server network. The hackers were then able to steal 40 million credit card records as well as other portions of critical customer information. Consequently, ***Target's sales fell by 46% in the final half of 2013[2]****, and the retail giant saw a 35-point drop[3] in its Buzz score (down to a -9). By May 2017, the breach had cost Target nearly $300 million[4] in legal fees and settlement negotiations. Consumer reports were fraught with mistrust and frustration.*

In 2014, Russian hackers used methodical infiltration and decryption tactics to penetrate Yahoo's network security. Through two consecutive breach attempts, the hackers compromised over 500 million[5] Yahoo accounts. After two years, the attack became public, and its stock immediately fell[6] by 5%. Another ramification of the breach was the necessary renegotiation of sale terms with Verizon who had been slated to acquire the web services provider. ***Yahoo was forced to take $350 million[7] off the original sales price to accommodate for the financial and socio-economic injury done to the brand.***



Data breaches are costly. And we don't just mean financially.

Most recently, in May 2017, hackers infiltrated the Equifax network through a web-app vulnerability that had a patch available in March earlier that same year.[8]

Unfortunately, the patch had not yet been applied, so hackers were able to access the names, birth dates, Social Security numbers, addresses, and driver's license numbers of more than 143 million[9] *US consumers. In a single afternoon, Equifax stock plummeted by 7.5%, with more recent numbers reaching an 18% drop.* ***Already, the breach has cost investors over $3.5 billion***[10]***, with more losses projected to come.*** *Despite Equifax's best efforts to mitigate losses and to offer free credit monitoring services to their end users, public distrust continues, and the Equifax brand suffers.*

Other side effects that companies suffer post-breach include:

- Legal liability (such as class action lawsuits)
- Reduced shareholder value
- Loss of partners/sponsorships
- Loss of customer base

The more data is lost, the higher the cost—and the more the company's brand loses credibility and favor. However, it is important to note that these three iconic breaches all occurred when Target, Yahoo, and Equifax already had active security measures in place.

If these organizations suffered hacks on their actively protected data, how much easier is it for cybercriminals to leverage data that is low-hanging fruit—when companies simply discard their equipment without taking the necessary security precautions?

It's your brand's reputation on the line. What are you going to do to protect it?

ACTIVELY PROTECT YOUR DATA—EVEN AFTER YOUR HARDWARE REACHES EOL

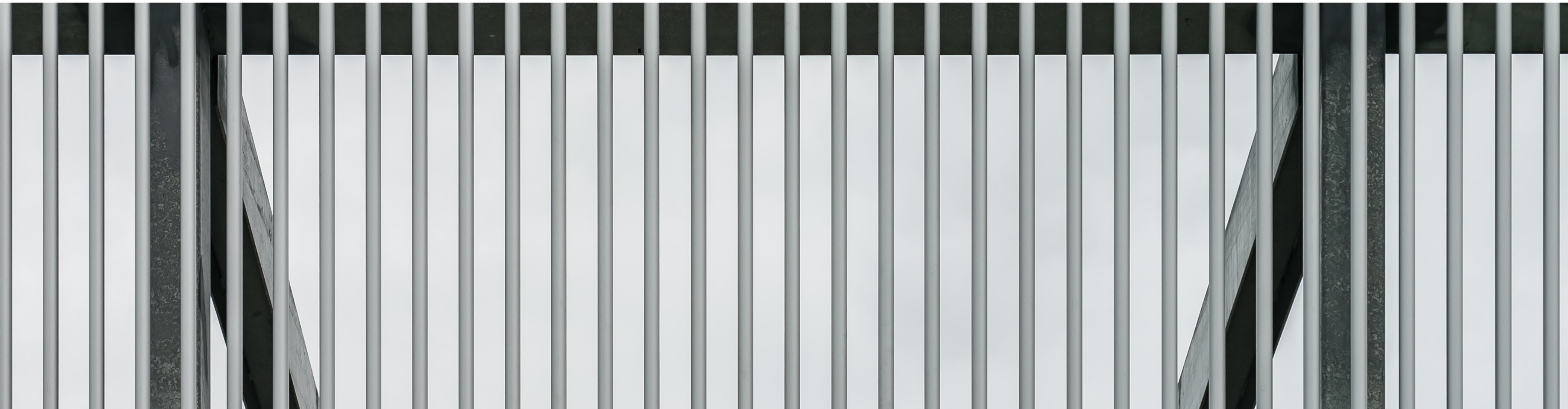
To ensure the reputation of your company's brand, your finances, and the safeguarding of your customers, you must sustain your security protocols until there is no data left to secure. No, this does not mean that you need to keep all iterations of hardware locked up in your data centers for all eternity. It simply means that, **as soon as any of your data leaves the protection of your network firewalls, you must immediately execute proper IT asset disposition (ITAD) measures.**

"ITAD" does not simply mean that you empty your recycling bin, re-image your hard drive, and have your IT team clean up the units before reselling or recycling them, however. **Data is intrinsically resilient—it tends to stick around—which can leave your company susceptible to breaches long after you have finished using the hardware.**

Unless you take the proper precautions.

Most likely, your company doesn't have the in-house specialization, the certifications, or the proper tools to manage end-to-end ITAD services, so you need a reputable vendor to complete the data protection process for you.

In order to make an informed vendor decision, you must first understand what a comprehensive approach to ITAD looks like.



THE ITAD PROCESS

ITAD services complete the lifecycle of end-to-end data security, with data sanitization being the first step toward its completion. Data sanitization can be accomplished in several different ways, but, depending on the situation, only specific methods will be effective. Consider the following scenarios.

DATA ERASURE VS. DESTRUCTION

Before you begin the decommissioning process, your hardware should be organized into one of three categories: resale, reuse, or recycle, and attention must specifically be paid to the type of hard drive that is housed in each unit. **Bear in mind that your data sanitization protocols—data erasure vs. destruction—are contingent on hardware compliance requirements and the future purpose of the equipment itself.**

DATA ERASURE:

Data erasure (or clearing/wiping) is a software-based process that completely overwrites the hard drive with random zeroes and ones, effectively obscuring any residual data left on the device under several layers of meaningless binary.

For DoD 522.20, the standard number of overwrites is 3, extended is 7 (two runs of DoD with an extra pass on top), and the “paranoia pass” is 21+, but the latter wears out the drive more quickly.

At CentricsIT, we leverage Blancco[11] erasure technologies for our clients’ data sanitization purposes. We understand the importance of comprehensive security, so we choose Blancco each time because its software satisfies most compliance requirements**, including DoD 5220.22 M and NIST 800-88 erasure methods.**

Wiping drives that are simply going to be recycled is obviously a wasted expenditure. As such, companies tend to only pay to erase hard drives that retain a feasible amount of secondary market value that can offset erasure costs. However, drives that are under restrictions like HIPAA, PCI, or FISMA often cannot be wiped per their compliance requirements; these drives must instead be destroyed.

DATA DESTRUCTION:

Data destruction is the physical process of making a hard drive unusable for conventional equipment. Arguably, this method can be accomplished with a hammer and some sweat equity, but this is an extremely inefficient method (especially if you have hundreds of units to decommission). Instead, most companies rely on punching and shredding machines to do the job.

Punching requires hand-drills or drill presses to punch holes into the drives to make them unreadable (although, plausibly, if not done correctly, data could still be gleaned from the drive). While this method is more effective with spinning disks, it is not as effective with solid state drives (SSDs).

> **Shredding** machines are similar to paper shredders, but they are built to accommodate more resilient materials. The machine's powerful, rotating teeth completely destroy the drive, leaving no possibility for drive or data reassembly. This method is ideal for all types of hard drives, but remains especially important for SSDs to ensure the destruction of each onboard memory chip.
>
> Because shredding is more comprehensive, CentricsIT encourages our clients to have their drives shredded rather than have them wiped (though we do offer punching services as well).

Data wiping is applied to units with residual market value, and data destruction is leveraged for economical and compliance solutions. As you well know, however, there is more to disposition compliance than data sanitization.

In some cases, it's all about the location.

ITAD PROCESSES: ON-SITE OR OFF-SITE?

Depending on your specific hardware, compliance, and budgetary limitations, you will need to decide whether to have your data sanitized on-site or off-site.

As with any decision, both sides will have pros and cons.

ON-SITE SERVICES: MORE EXPENSIVE BUT FASTER AND MORE SECURE

Some companies choose to conduct data sanitization on-site because of the additional oversight it enables.

When asked to perform on-site data sanitization, ITAD technicians bring all the necessary equipment with them—wiping software, shredders, and their expertly-honed processes. As a result, your hardware does not leave the premises until it has been completely stripped of its former data. While the on-site method is more secure, it also offers a few challenges that you should consider.

On-site services:

- Can be difficult to schedule as delivery time varies with volume, procedure, and accommodations.
- Require a secure, open space in your data center for ITAD technicians to operate machinery and run software.
- Require power, cooling, and a separate, dedicated network (for data erasure*).
- Are more expensive than off-site services due to the logistics, tools, time, and dedicated manpower needed to execute them.

**More specifically, when you choose on-site for data erasure, you will not only need a physical space in your production environment, you will also need an off-line, dedicated local area network (LAN) for technicians to run the Blancco software. Due to the limited space and the temporary nature of the LAN, the number of units that can be erased concurrently is limited as well.*

CHOOSING THE RIGHT PEOPLE FOR THE JOB

EVERYONE'S AN ERASER

Practically anyone in the tech industry can download free software (like DBAN) and offer “data erasure,” but they likely lack the legal certifications to validate their services. Most free software does not come with the industry certifications and guarantees of a vetted provider like Blancco. You will still be liable for the fallout if a breach occurs (due to incompetence on the vendor's part or an unpatched bug in the software that was used, etc.).

Our experts report that, **12-15% of the time, they find end user data on devices that have been marked as “clean” in the secondary markets.** This occurrence can happen due to incompetence, apathy, or outright laziness from a vendor—don't blindly trust your data sanitization process, only to end up as the next big data breach on the world's newsfeed.

DOING RECYCLING THE RIGHT WAY

Mom-and-pop shops will offer “e-cycling” services at a bargain price, especially within smaller markets. If they cannot offer you legal documentation—or if they don't have the proper **ISO or R2** certifications to guarantee your hardware's proper recycling and disposal—you will face the legal ramifications if your servers end up tossed in a landfill or left to gather dust in an abandoned warehouse.

At CentricsIT, we take pride in our certifications[13], and we work diligently to meet those requirements year after year. Not only that, we insist on maintaining downstream partners who do the same. As such, our clients rest assured that their hardware is properly disposed of and their compliance stricture will be met, according to our zero-landfill policies and our ISO and R2 regulations.

(BREAKING) THE CHAIN OF CUSTODY

The shipment process can also be fraught with incompetency if you choose the wrong vendor for off-site data sanitization processes. It is essential when transporting units with residual data to maintain chain of custody from the time the hardware leaves your facility to the second that the data is overwritten. If you choose vendors without certified shipping services and methodologies, then you run the risk of hardware theft and subsequent data breaches.

CentricsIT provides secure chain of custody for every hardware shipment by default, and we have documentation, physical parameters, and fail-safes to prove it.

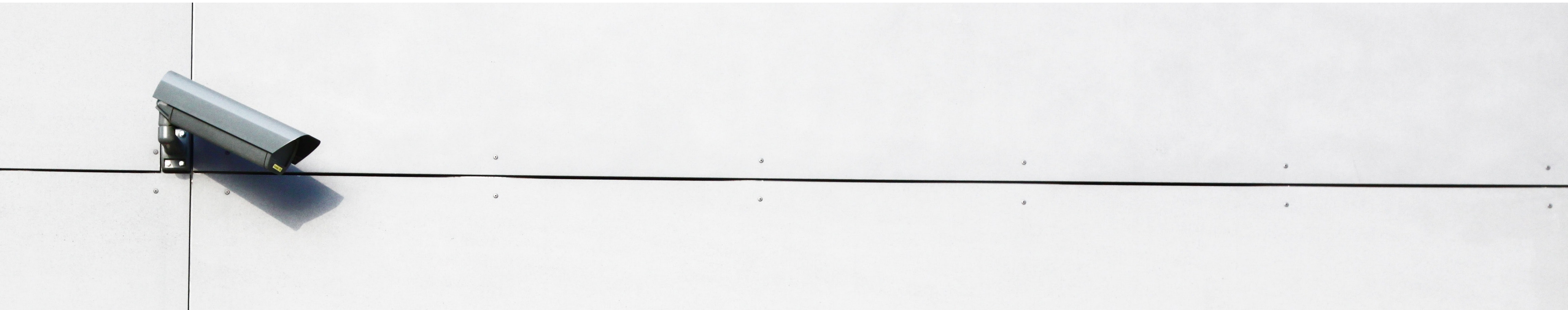
> Upon arrival, your units are carefully packed in Secure Transportable Units for Data Destruction, or "STUDD" for short (see our website[14] for more details). This lockable bin securely contains your data-bearing units from your facility to ours, with each lock being uniquely identifiable.

> The STUDDs are then loaded into point-to-point, dedicated trucks; "dedicated" meaning that the truck does not stop or pick up other clients' units along the way. Our drivers are highly-vetted and experienced within the industry.

> Each truck is cable-sealed with a serialized lock. Our drivers (and you) will know immediately if there has been unauthorized access.

> Pictures are taken throughout the entire shipment process to provide physical evidence of comprehensive security statuses. Our technicians take pictures of each locking mechanism before we leave your data center. Pictures are taken if/when drivers are relieved. Final pictures are taken upon arrival at our warehouse.

If your vendor is unwilling to provide you with the proper documentation and empirical assurances, don't hire them. Partner with an ITAD expert that can provide the proper documentation and procedures to guarantee your data (and your brand's) security from end-to-end.



A FEW MORE ELEMENTS TO CONSIDER POST-DECOM:

Data sanitization and brand protection measures may not be as expensive as you think. We discussed briefly the price differences between data erasure and destruction; however, what some people fail to understand is the extent of the latent value that can be reclaimed from decommissioned hardware. In some cases, the proceeds made in secondary markets can counteract, if not pay for, the decom expenses themselves.

(Interested in finding the hidden value in your assets? Check out our recent e-Book, *A Smarter Way to Hybrid Cloud.*)

As we mentioned earlier, be sure to collect a Certificate of Destruction (CoD) from your data sanitization vendor. But remember, if a breach occurs, the general public doesn't care about a signed piece of paper, no matter how legitimate it may be. Your brand will still be the one that predominantly suffers the consequences (which is why you should partner with trustworthy vendors). Your process—and the process of your chosen vendor—is what really keeps you safe.

Remember that even something as seemingly insignificant as asset tags can negatively reflect on your company, especially if you choose a vendor with apathetic security processes. Some data sanitization vendors might gloss over those smaller details, but, to the experts at CentricsIT, no measure is too trifling. As such, our technicians meticulously remove and destroy every asset tag (in addition to providing you complete data erasure and destruction services). A piece of hardware is not clean until is it is stripped of all identifiable data.

Following these practices should ensure your data security and brand protection. When you decommission your IT assets properly, the risk of data breach decreases significantly, and so does the risk to your brand reputation.

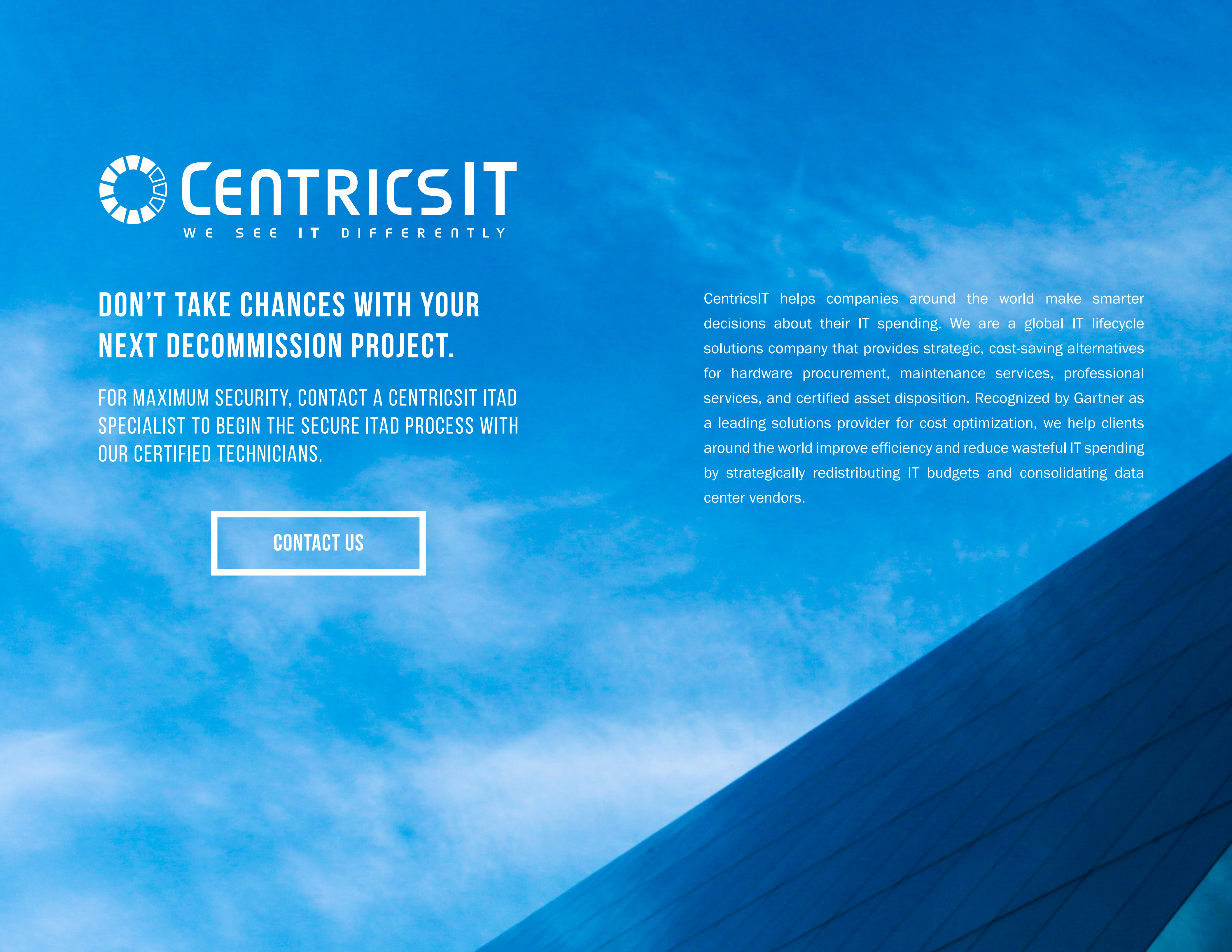
PROTECT YOUR BRAND: DECOM THE RIGHT WAY

With any IT asset decommissioned project, CentricsIT determines which option is best for your business and deploys advanced disk sanitization methods to erase your data to HIPAA and Department of Defense NISPOM standards or uses disk destruction devices to obliterate your hard disks entirely with data erasure. Regardless of the procedure you choose, CentricsIT provides you with a Certification of Erasure or Destruction, backed by our data security guarantee. And all of our IT recycling practices meet or exceed EPA standards.

No matter how established a company, **a single hack can devastate its brand for the foreseeable future.** Why invite such attacks by not protecting your data through its entire lifecycle?

Managing the complexities of comprehensive security takes time and experience. You can't do it alone. Contract with a vendor that can empirically prove its diligence and capabilities through legal documentation, certifications, and vetted protocols. CentricsIT provides these assurances for our clients. Not only that, we are willing to be transparent; we welcome accountability where other vendors will not. If you want to see the procedures for yourself at any point in the disposition, we will walk you through the entire process and our methodologies. We have nothing to hide.

We know how to do ITAD right the first time. **With a data breach, you don't get a second chance.**



CentricsIT

WE SEE IT DIFFERENTLY

DON’T TAKE CHANCES WITH YOUR NEXT DECOMMISSION PROJECT.

FOR MAXIMUM SECURITY, CONTACT A CENTRICSIT ITAD SPECIALIST TO BEGIN THE SECURE ITAD PROCESS WITH OUR CERTIFIED TECHNICIANS.

CONTACT US

CentricsIT helps companies around the world make smarter decisions about their IT spending. We are a global IT lifecycle solutions company that provides strategic, cost-saving alternatives for hardware procurement, maintenance services, professional services, and certified asset disposition. Recognized by Gartner as a leading solutions provider for cost optimization, we help clients around the world improve efficiency and reduce wasteful IT spending by strategically redistributing IT budgets and consolidating data center vendors.

SOURCES

[1] Krebs, Brian (2014). "Target Hackers Broke in Via HVAC Company." Krebs on Security. krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[2] Drinkwater, Doug (2016). "Does a Data Breach Really Affect Your Firm's Reputation?" CSO Online. www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html.

[3] Marzilli, Ted (2013). "Target Perception Falls After Data Breach." YouGov BrandIndex. www.brandindex.com/article/target-perception-plummets-after-data-breach.

[4] Lynch, Vincent (2017). "Cost of 2013 Target Data Breach Nears $300 Million." Hashed Out. www.thesslstore.com/blog/2013-target-data-breach-settled/#_ftn1.

[5] Newman, Lily Hay (2017). "Hackers Breach a Billion Yahoo Accounts. A Billion." Wired. www.wired.com/2016/12/yahoo-hack-billion-users/.

[6] Reuters (2016) "Here's How Much Yahoo Shares Are Dropping After Latest Hack Reveal." Fortune. fortune.com/2016/12/15/yahoo-shares-hack/.

[7] Paul, Fredric (2017). "We Finally Know How Much a Data Breach Can Cost." TechWatch. www.networkworld.com/article/3172402/security/we-finally-know-how-much-a-data-breach-can-cost.html.

[8] Newman, Lily Hay (2017). "Equifax Officially Has No Excuse." Wired. www.wired.com/story/equifax-breach-no-excuse/.

[9] Hall, Christine (2017). "How Much Will the Data Breach Cost Equifax?" Data Center Knowledge. www.datacenterknowledge.com/business/how-much-will-data-breach-cost-equifax.

[10] Kilgore, Tomi (2017). "Equifax's Data Breach Costs Investors a Lot More Than It Will Cost the Company." MarketWatch. www.marketwatch.com/story/equifaxs-data-breach-costs-investors-a-lot-more-than-it-will-cost-the-company-2017-09-11.

[11] Blancco (2017). "The Most Certified Data Erasure Solutions in the World." www.blancco.com/about-us/supported-standards/.

[12] "Millions of lead-filled CRTs have been abandoned in warehouses across America" (2017). BoingBoing. https://boingboing.net/2017/02/17/millions-of-lead-filled-crts-h.html

[13] "Quality Certifications: Why They Matter" (2017). CentricsIT. www.centricsit.com/quality-certifications-why-they-matter/.

[14] "[STUDD] Secure Transportable Unit for Data Destruction" (2015). CentricsIT. www.centricsit.com/studd-secure-transportable-unit-for-data-destruction/.