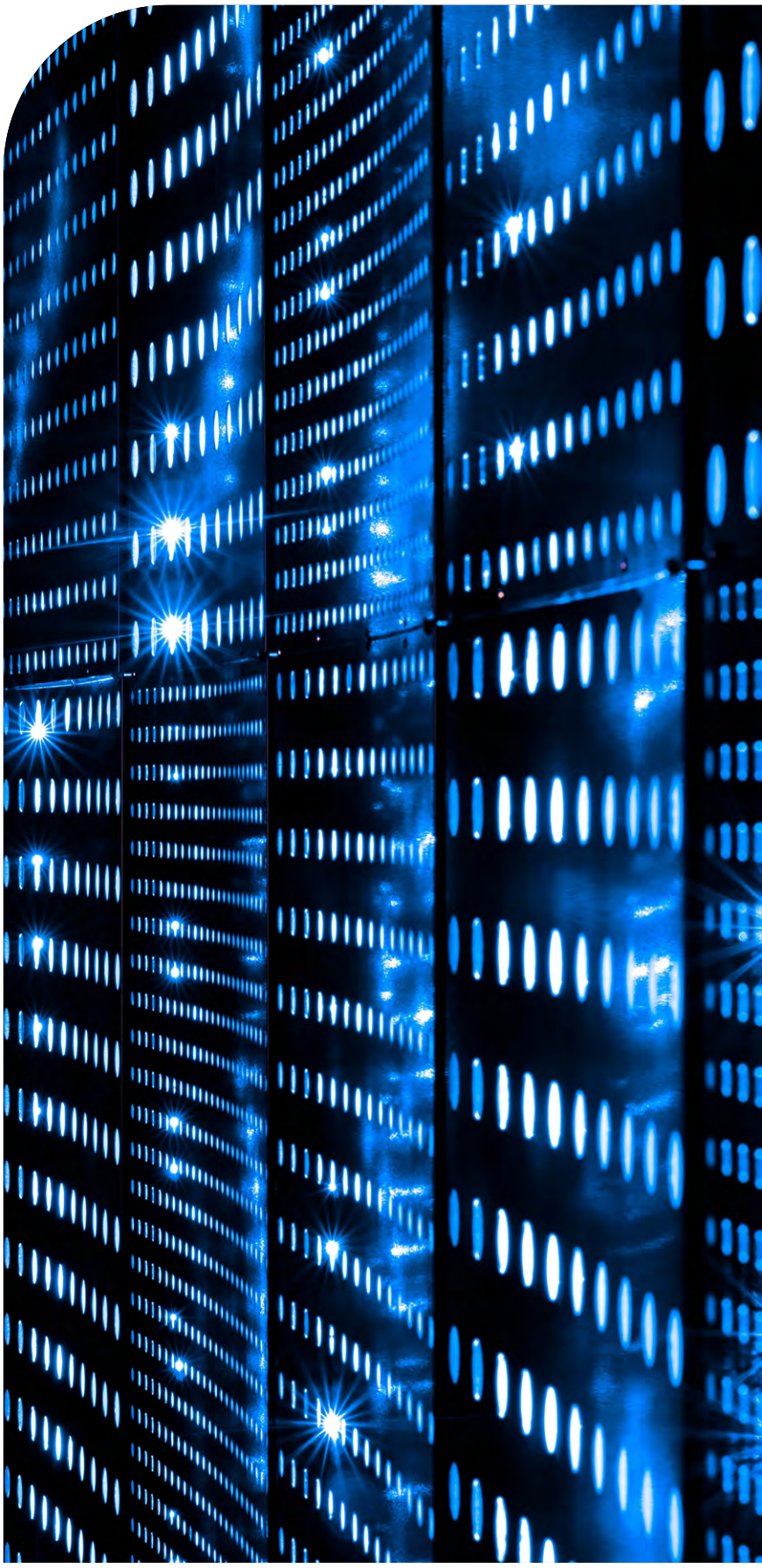
GOVINSIDER

IN PARTNERSHIP WITH

blancco

GUIDE TO SECURE DATA DISPOSAL



FOREWORD

Yogesh Hirdaramani
Reporter, GovInsider

In antiquity, Romans would write on wax-covered tablets that could only be erased by heating the wax to smooth it over. This is the origin of the phrase 'tabula rasa' – a clean slate. In a time when paper was expensive, these reusable surfaces became the preferred medium to write in.

In today's digital world, hard drives and solid-state drives are some of the most common ways in which governments and businesses record information across all verticals. Yet, even as the threat of critical data breaches looms over agencies worldwide, the pressing needs of the climate crisis means that agencies are seriously exploring ways to reduce carbon emissions and e-waste, reuse resources, and recycle hardware.

If we can restore IT assets to tabula rasa, can secure data disposal methods help agencies tackle these twin challenges?

This guide shares insights, case studies, and features on the ways governments are addressing sustainability goals and securing their data practices. It will take you on a journey through the myriad projects governments in Southeast Asia are embarking on to manage e-waste, strengthen cybersecurity practices, and address data governance matters.

We're thrilled to be working with Blancco, a leading data security company that specialises in data erasure and computer reuse for corporations, to share their expertise. Throughout the guide, voices from Blancco will highlight how secure data disposal can advance government ambitions to mitigate the climate crisis while strengthening their confidence in their data governance.

Happy reading!

Masayuki Morita
Vice President of Blancco APAC

Governments and public sector agencies worldwide are gathering, generating, and storing more digital information than ever. Defense projects, government apps, healthcare and infrastructure initiatives contribute to a staggering amount of data collection and processing.

Naturally, such processing requires an extensive amount of physical hardware. Yet the increasing amount of data-laden hardware creates risk for both data security and the environment.

Government IT assets are typically refreshed every 3-5 years, creating a "security vs. sustainability" dilemma when it comes to disposing of it. The traditional approach of destroying used technology in the name of data security has produced a glut of electronic waste. It also leads to an increased depletion of natural resources, and strained fiscal budgets: In Japan alone, an estimated annual public sector spend of more than $4.5M goes to solid-state drive (SSD) destruction and replacement, with more going to destroying and replacing magnetic hard disk drives (HDDs).

Yet there's no question that sensitive data—whether from local employee devices, on-prem or remote data centres, or the cloud—must be protected.

The good news is that data security doesn't have to work against environmental goals. Quite the opposite. By looking at device disposal differently, IT asset managers and infosecurity officers can more fully support global, national, and local calls for greener government operations. At the same time, they can actually increase levels of data protection while cutting costs. The key is to make that data absolutely irretrievable, freeing devices for extended use.

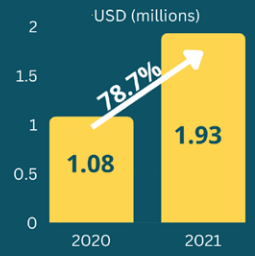
Erasing data is a financially prudent, efficient, and regulation-compliant practice adopted by security-conscious agencies and industries around the world. To find out how data erasure is used in agencies worldwide, please contact me directly at masayuki.morita@blancco.com.

TABLE OF CONTENTS

Secure data erasure at a glance:
The costs of device destruction and its alternatives

1

Average cost of a data breach in the public sector



Data breaches can come from anywhere, including end-of-life.

This year alone, a well-known US investment bank agreed to pay **US$60 million** to settle a lawsuit over a personal data breach allegedly caused by improper disposal of data-bearing assets.

Is secure data erasure a solution?

An independent research company surveyed nearly 600 public sector employees around the world to find out how it compares to device destruction.

2

Costs of device destruction

Nearly
US$60 million
is spent annually destroying and replacing SSD devices amongst the respondents

Roughly one SSD is destroyed for every 3 employees annually, cutting short device life and reuse options

93% plan to reduce the environmental damage caused by device destruction

but

less than a quarter are implementing them

3

Why do people still destroy devices?

46% believe physical destruction is more secure than other solutions

but only

13% strongly agree they have full confidence in their organisation's physical destruction process

22% were unaware of **alternative methods of data disposal**

4

Why data erasure?

Render data completely inaccessible against sophisticated laboratory attempts

Seal gaps in chain of custody processes

Provide immediate verification and certification that data has been rendered irretrievable

Allowed for by **internationally referenced data protection guidelines**

Securely erasing and redeploying just one laptop can prevent the release of **258 kg of CO2** — equivalent to **304 km traveled by a heavy goods vehicle**

Learn from the best: Highly advanced digital government agencies like Singapore's Government Technology Agency are already **adopting Blancco's data erasure software to sanitise data in ways that preserve the device for reuse**

Sources: IBM Cost of a Data Breach Report 2022 | The Price of Destruction: Exploring the Financial and Environmental Costs of Public Sector Device Sanitisation, March 2022 | Carbon Handprint Guide, 2018

Back to Table of Contents

How Singapore is working with industry players and citizens to recycle electronic waste

By Woo Hoi Yuet

Interview with Ron Wong, Director (Waste Management Division) at the National Environmental Agency, on how Singapore is solving the electronic waste problem.

In the movie Wall-E, a lone robot roams an Earth that has been left in rubble. It's no longer skyscrapers lining the sides of the pavement—huge mountains of trash tower over us instead.

That might sound like a dystopian future. But it shows us what our future could look like if we don't confront our waste problem. E-waste is one of the fastest-growing waste streams on Earth, with the world discarding at least $62.5 billion worth of e-waste annually, the World Economic Forum reported. That's more than twice of Cambodia's current GDP.

How can governments help to reduce e-waste? Ron Wong, Director of the Waste Management Division at the National Environmental Agency (NEA), shares how Singapore works with industry players and citizens to recycle electronic waste.

Buried in e-waste

Singapore generates around 60,000 tonnes of electronic waste (e-waste) annually. That's equal to each person in Singapore throwing away 70 mobile phones, NEA said.

If we don't decrease the e-waste that we produce, it's not only the heap of trash that piles up. We are also exposing ourselves to more health risks.

When e-waste is burnt, it releases toxic fumes that increase the risk of respiratory illnesses. Harmful metals and chemicals used to make electrical products can also seep into the soil and pollute waterways.

We are also running a race against time. The e-waste problem further places pressure on Singapore's limited resources and waste management infrastructure like landfills, Wong shares. Singapore's only landfill, Pulau Semakau, will be filled by 2035, the Ministry of Sustainability and the Environment (MSE) reported.

"It's important for us to shift from a linear economy to a circular one," Wong highlights. Resources are reused endlessly in a circular economy. Instead of going straight to the landfill, they are given new lives by being turned into other products.

Partnering industry players

Singapore's Zero Waste Masterplan, which aims to reduce the amount of waste by 30 per cent by 2030, has identified e-waste as a key focus.

To do so, Singapore brought together industrial players—producers, retailers, and recyclers—to "co-create an e-waste EPR (Extended Producer Responsibility) system tailored to Singapore's needs," Wong shares. This means that those producing and supplying electronic products are responsible for ensuring that e-waste is recycled in an environmentally sustainable manner.

Producers, who supply or produce electronic products to retailers, have to finance how the e-waste is properly collected and recycled. In Singapore, they pay a fee to an e-waste recycling company, ALBA E-Waste Smart Recycling, to recycle the products for them.

Retailers, who sell the products directly to consumers, are required to bring the old electronic products to the recycling centres upon delivering the new products, Wong adds.

For example, when you buy a fridge from a retailer and get it delivered to your house, you can ask the retailer to take back your old fridge at no cost. The retailer will then pass the old fridge to the e-waste recycling centre, whose services are paid for by the producer, Wong explains.

"As the system matures and people are more aware, we expect the amount of e-waste collected to increase," Wong highlights. Since producers are paying for the recycling of electronic products, the EPR system will also attract more e-waste recycling companies to set up in Singapore.

Engaging citizens

Beyond industrial players, citizens can play a huge role in managing e-waste too. Only one in ten young Singaporeans recycle e-waste. Out of those, three in ten throw e-waste in the wrong bin, a survey revealed.

NEA has been raising citizen awareness about e-waste recycling. For instance, it provides a map of the 500 e-waste recycling bins in Singapore on its website. ALBA also organises quarterly collection drives four times a year at housing blocks. Residents can also collect points and redeem prizes whenever they recycle their electronic products at ALBA's e-waste collection points.

An important step toward sustainability is also to reduce the amount of e-waste going into the bins in the first place. When our electronic products are spoilt, we can consider repairing them instead of throwing them away and buying new products.

Repair Kopitiam, a community-based initiative, aims to create a more sustainable mindset amongst consumers. Volunteers teach residents how to fix their broken electronic products free of charge.

It also organised the #EWASTENOMORE challenge in 2021 with SGTECH, a trade association for Singapore's tech industry, encouraging citizens to invent a new product using parts from broken electrical appliances.

Through supporting these initiatives, NEA hopes to "rally everyone to come together and play a part in Singapore's aim to become a zero-waste nation," Wong shares.

Success stories around the world

Since the start of NEA's EPR scheme in July 2021, ALBA has collected 3500 tonnes of e-waste, Grace Fu, the Minister of MSE, reported. This is thrice as much as NEA's previous voluntary partnership with industrial players to recycle e-waste.

The movement to reduce e-waste is gaining traction in other countries too. Reboxed, a London startup, allows users to buy, sell or swap second-hand mobile phones instead of tossing them straight into the landfill.

There are also exciting innovations in tackling the e-waste problem. Scientists from the National Technological University (NTU) in Singapore used fruit peels to extract precious metals from disposed batteries, which can then be used to create new batteries.

While Wall-E's reality depicts an abandoned, trash-filled world, our Earth's future has not been set in stone yet. "With a proper system, we can prevent negative impacts to the environment," Wong emphasises. The government, industrial players, and citizens must work together to reduce e-waste.

Back to Table of Contents

How government agencies can lead the way in reducing e-waste

By Blancco

Fredrik Forslund, Blancco Vice President of Enterprise & Cloud Erasure Solutions, shares how government agencies can limit the flow of e-waste.

The Agbogbloshie scrap yard in Ghana is home to 80,000 residents who subsist by breaking up e-waste to recover metals. But any adult who eats a single egg laid by the free-range chickens who reside there would expose themselves to a dangerous level of toxic chemicals, reported The Guardian.

This scrap yard is one of many places around the world where poorly disposed e-waste goes to fester, leaking poison and toxins into food, water, and soil. In 2021, the world generated 57.4 million tons of e-waste, outweighing the Great Wall of China. Government agencies can set a better tone for industry and society by committing to reducing e-waste.

Fredrik Forslund, Blancco Vice President of Enterprise & Cloud Erasure Solutions, shares how government agencies can lead the way in reducing e-waste by erasing data securely with software, making full use of existing IT equipment, and setting regulations.

Erasing data securely with software

One way to extend the life of IT devices is through erasing data with software rather than relying on physical destruction to remove sensitive data, shares Forslund.

E-waste that is not properly disposed of can affect the environment by releasing cancer-causing toxins into the air. It can also contaminate soil with heavy metals that can make their way into ponds and seawater, endangering marine life and our oceans.

Physical methods of destroying IT devices to remove data, such as drilling holes, melting, and burning, can release such toxic chemicals. In contrast, data erasure can securely remove sensitive data without harming the environment, while allowing the equipment to be reused.

The overwhelming concern regarding reusing media storage devices is security, notes Forslund. 46 per cent of 596 public sector respondents in a Blancco survey shared that they chose to physically destroy drives as opposed to other methods to maintain security.

However, depending on how it's done, physical destruction does not guarantee that data is irretrievable, explains Forslund. Forensic teams may still be able to recover data from seemingly destroyed drives. Agencies can instead adopt software-based methods to render data inaccessible against sophisticated laboratory techniques and run third-party tests to certify that data is completely erased.

Physical destruction should only be a last resort, emphasises Forslund.

When an asset does come to the end of it's useful life, agencies should also try to recycle materials to the best of their abilities, rather than simply disposing of them, he suggests. For instance, the rare metals that power hard drives can be recovered for future applications even when hard drives have reached end of life.

When agencies verifiably wipe data clean and reuse data storage drives, they can also save money. According to the public sector survey, government agencies with more than 1,000 employees are each spending between US$21,495 and US$28,660 a year on average destroying solid-state drives. If agencies reuse rather than destroy drives, they can reduce this figure significantly.

Make full use of existing IT equipment

Government agencies can endeavour to make full use of existing IT equipment, shares Forslund. They can do this by putting a stop to the unnecessary destruction of IT assets in the name of data security and reusing IT equipment like solid-state drives.

"Everything comes with a carbon footprint", notes Forslund. From production, packaging, to shipping, IT equipment like solid-state drives arrive at an agency's doorstep having already generated a sizable carbon footprint, he explains.

When agencies discard IT equipment prematurely to ensure that sensitive data is not accessible, they add on to this carbon footprint. Then, IT companies expend more resources to produce new equipment, generating even more carbon emissions.

Respondents in the Blancco survey reported that, collectively, they spend between US$12.8 million to US$17 million each year destroying solid-state drives, and another US$40 million replacing them, shares Forslund.

Organisations annually dispose of roughly one solid-state drive for every three employees, refreshing technology every three to four years, even while devices are still functional. Devices that are destroyed have their useful life cut short, and redeployment, resale, and return options are no longer possible – wasting the device's potential for reuse.

In Australia, Blancco is partnering with Ethan Indigenous, an ICT service provider that delivers opportunities to Indigenous Australians, to support the donation of used government and enterprise laptops to Indigenous youth who lack access to the Internet. Blancco helps securely erase drives and laptops, ensuring that previously stored data is rendered inaccessible.
SGTech, Singapore's leading trade association for the tech industry, has also been supporting repair and reuse efforts, shared GovInsider. Their 2021 #EWASTENOMORE challenged the public to find innovative ways to upcycle or repair faulty household appliances. They have also been running a series of repair demonstrations online to encourage a culture of repair and reuse.

Set regulations

Finally, government agencies can set regulations to reduce e-waste and promote recycling.

Countries around the world have released green plans, from Singapore's Green Plan, to the United States and Canada's Greening Government Initiative. These plans signal a commitment to climate action by aiming to reduce carbon emissions, swap to renewable energy, and reduce waste.

Blancco's research survey found that 93 per cent of public sector respondents have clear plans to reduce the environmental impact caused by destroying IT equipment. However, less than a quarter are actively implementing these plans.

One example of an agency putting these plans into action is Sweden, shares Forslund. The Swedish government's National Agency for Public Procurement is encouraging sustainable procurement through a set of sustainability criteria. This includes encouraging contracting authorities to purchase from suppliers that provide a reuse and recycling service for worn-out IT equipment.

As e-waste becomes a more pressing problem globally, governments can take the first step to encourage a culture of responsible consumption, by erasing data securely with software, making full use of equipment, and setting regulations.

Back to Table of Contents

How Malaysia is securing its critical data

By Ranamita Chakraborty

Dr Maslina Daud, Senior Vice President, Cyber Security Proactive Services Division, CyberSecurity Malaysia, shares how Malaysia is securing its critical data and disposing of them safely.

Costa Rica recently declared a state of emergency after a major ransomware attack. Hacking organisation Conti exploited gaps in the country's public cybersecurity infrastructure to steal sensitive data and demand a US$20 million ransom. This disrupted government services and digital public platforms for over a month.

It is clear that a new age of catastrophic cyberattacks has begun. It is critical for government and private sectors to bolster their cybersecurity approaches as threats escalate. This is where CyberSecurity Malaysia plays a crucial role in developing Malaysia's cybersecurity environment as the country's reference centre for cybersecurity.

Dr Maslina Daud, Senior Vice President, Cyber Security Proactive Services Division, CyberSecurity Malaysia, shares Malaysia's cyber defence approach for securing critical data and disposing of them safely.

A proactive approach to cybersecurity

First, it is important for organisations to be proactive in managing their cybersecurity so they can be resilient to cyber threats, says Daud. Organisations typically take cybersecurity matters seriously only after they have been attacked or after security breaches occur.

New tech such as AI, IoT devices, and 5G have created a risky environment for organisations to operate. For instance, AI systems can be compromised and data from IoT devices running on 5G could leak easily without authentication mechanisms in place, says Daud.

As the head of the Proactive Services Division, Daud's role is to assure trust and confidence in the Malaysian cybersecurity space. Her team works to prevent cybersecurity breaches and minimise impacts should they occur.

To counter cyber threats, organisations can implement a variety of security measures. These include conducting risk assessment exercises consistently and reviewing security logs regularly, explains Daud. Through such measures, organisations can minimise chances for cyber attackers to exploit system weaknesses.

Data classification protects data

Second, classifying data correctly is a key way organisations can better secure critical data. It allows them to know the value of their data and understand the implications of data corruption or loss. It also helps them comply with data protection requirements set forth by their regulatory bodies.

Data classification is one of the listed cybersecurity controls under the international standard Information Security Management System (ISMS). It categorises data based on its type, sensitivity, and value to the organisation. Methods like modifying sensitive data and data encryption can protect different types of data.

Different classes of data require different levels of protection. When data is underclassified, it leads to insufficient protection and when it is over classified, unnecessary costs are involved in protecting them. Having a full understanding of data allows organisations to protect them from threats, says Daud.

Secure data disposal

Next, it is also important to destroy sensitive data in a secure way because data owners are put at risk if such data is not disposed of properly. Organisations may handle data that is no longer required differently depending on how securely classified the data is. They usually perform physical destruction when disposing of data, says Daud.

However, it is crucial for organisations to establish their own security processes when dealing with third parties that are contracted to perform data disposal, notes Daud. These processes need to provide a high level of assurance that the data is no longer readable and accessible.

Best practices for cybersecurity

Finally, organisations can adopt best practices in cybersecurity by adhering to security guidelines, says Daud.

For instance, government agencies in Malaysia observe guidelines on information security management for cloud computing issued by the Chief Government Security Officer's Office. These guidelines include recommending agencies to perform risk assessment for understanding possible security risks and implementing security controls to mitigate them.

Additionally, government agencies refer to the National Trusted Cryptographic Algorithm List also known as MySEAL to securely encrypt data, shares Daud.

Upcoming security projects

CyberSecurity Malaysia is currently seeking to instill trust and confidence among the public on biometrics and digital identity initiatives. The agency is working on data projects evaluating biometric security for mobile devices which is focused on personal verification and remote authentication capabilities, shares Daud.

The agency is also coming up with a blockchain security assessment initiative which could allow organisations to fix any potential weaknesses in their blockchain-based applications, she adds.

In this age of sophisticated cyberattacks, it is crucial for organisations to take a proactive approach to cybersecurity and govern it properly. They can do so by classifying critical data, disposing of data securely and adhering to security guidelines. Such practices can help them mitigate and detect cyber attacks and threats efficiently.

Back to Table of Contents

A false sense of security: why physical destruction of data cannot ensure cybersecurity

By Blancco

Fredrik Forslund, Blancco Vice President of Enterprise & Cloud Erasure Solutions, shares how government agencies can securely dispose of data with software.

Many believe that complex passwords with special characters are the most secure. Yet, in 2021, the United States Federal Bureau of Information recommended opting for longer "passphrases" comprising multiple words strung together, as these are harder to crack.

Agencies must always evaluate commonly used best practices as time passes and new knowledge emerges. Nowhere is this truer than data disposal. Many government agencies and private companies around the world believe that physical destruction of data storage media is the most secure way to dispose of data, but software-based data destruction may be safer.

Fredrik Forslund, Vice President of Cloud & Data Center Erasure, Blancco, shares how government agencies can best secure their data by destroying data with software, automating data disposal, and improving awareness of current data security standards.

Adopt software-based data destruction

Contrary to popular belief, government agencies can best secure their data by using software to destroy data rather than opting for physical destruction, shares Forslund.

A recent survey of 596 public sector respondents found that physical destruction is considered more secure than other solutions by 46 per cent of respondents globally. Physically destroying data storage devices, such as solid state drives and hard disks may feel more reassuring, Forslund notes.

However, physical destruction is only effective when done in specific ways. For example, solid state drives need to be completely shredded to two to three millimeters in size. Otherwise, a forensic lab may be able to "recreate data from the electronic chips", he explains. Common methods like drilling still leave precious data vulnerable to data recovery efforts, he warns.

In fact, while 46 per cent of respondents stated that they physically destroy drives because it is more secure than other solutions, only 13 per cent strongly agreed that they have full confidence in their organisation's physical destruction process.

Software-based data destruction can induce a permanent "purge" state, shares Forslund. Once an agency has purged data from a hard drive, the data removal is equivalent to if they had shredded it, he explains.

"It doesn't matter what information you had on there. It's all gone and it can never come back," Fredrik Forslund, Vice President of Cloud & Data Center Erasure, Blancco, says.

Government agencies and private organisations may send sample drives to forensic laboratories in order to get a certificate of destruction, he adds. This can ensure that data is totally removed from the drive and alleviate any doubt.

When data is destroyed with software rather than with physical methods, the equipment will not have to be retired prematurely. As such, agencies can reuse these storage devices and maximise their full use. This can lead to environmental benefits and cost savings, as highlighted in a recent GovInsider article.

Automate data disposal

Software-based data destruction can also be automated, thereby reducing the risk of human error, says Forslund.

When sensitive data is no longer in use, it needs to be disposed of immediately, he highlights. Any delay can lead to excess vulnerability as long as the device retains data. Gaps in a device's chain of custody, which tracks the movement and control of a drive or device until ultimate destruction, also create risk.

For physical destruction to work, you need a perfect chain of custody, he explains. "Over and over, we've seen different data leaks [during this process], as employees or contractors are simply removing some of the drives to sell privately," he shares.

This tracking and documentation can be easily comrpomised when handling many devices. For instance, an agency that needs to destroy 12,000 drives would need to scan the serial number of each drive and collect proof that every drive has been shredded correctly.

The UK's NHS Digital had to record 393 missing devices over a year, even though they had processed 319 of them for disposal. As they had no record of disposing of those devices, all of them had to be officially listed as lost, along with the data stored on them.

An automated system can enable immediate sanitisation and generate an audit trail, he highlights. This can plug the gaps in chains of custody. Automated systems can generate reports tagged to each serial number to verify that all drives have been wiped via software.

A Japanese prefecture recently revised its procedures to seal gaps in its chain of custody process, following the loss of 18 hard drives destined for destruction. To protect against future data leaks, employees must witness onsite data erasure before storage devices are either reused or physically destroyed.

Improve awareness of data security standards

Agencies need to increase awareness of current data security standards and reform outdated policies, he shares.

When revising these processes, agencies "need to go from partial awareness to full awareness because you need every stakeholder to participate", he explains. In complex environments like government agencies, many different stakeholders need to be on the same page so that existing policies can be modified.

So, what's stopping government agencies from making the switch?

First, there is a lack of awareness of options. Blancco's research study found that 38 per cent of respondents globally say they do not have the appropriate skills in house to use other methods. Almost a quarter were unaware of alternative methods of data disposal, such as certified data erasure.

Secondly, there's a mismatch between policy and today's ambitions, shares Forslund. Many data disposal policies were written 10 to 15 years ago and have not kept up with the latest advancements in technology.

But it is not too late to revise policies. One country's department of defense that mandated the destruction of all solid state drives recently rewrote policy and mandated secure data sanitisation through Blancco software after looking into the department's processes, highlighted the research study.

Blancco's software has been certified by various public sector organizations focused on cybersecurity, such as the United Kingdom's National Cyber Security Centre, the German Federal Office for Information Security, and the Swedish Armed Forces.

As a critical mass adopts secure software-based data sanitisation, public sector agencies can be confident that data security has progressed past the need for physical destruction. With software-based data destruction, automated data disposal, and increased awareness of options, it is more secure than ever to make the switch.

Back to Table of Contents

Privacy-enhancing tools may offer a way out of a difficult digital dilemma

By Yogesh Hirdaramani

Conventional wisdom holds that data privacy is incompatible with the levels of convenience people have come to expect in their app-assisted lives. Initiatives in Singapore and Estonia are attempting to turn that notion on its head.

Few would dispute that the current moment in history is epoch-defining when it comes to the uses of digital data in people's everyday lives. Data undergirds our existence in ways that not so long ago were regarded as the stuff of science fiction. Yet amid all the convenience afforded by the digital assistance we receive through new tools and technologies, has privacy inevitably become collateral damage?

Tech giant Apple last year updated the operating system iOS 14 to allow users to opt out of sharing their data with advertisers on third-party platforms such as Facebook. The effect was immediate. According to Forbes, the move was related to a potential loss of US$10 billion of ad sales by Facebook owner Meta – nearly 8% of the company's annual revenue.

The Apple case demonstrates that as data privacy practices and regulations shift, companies and agencies will also have to shift their strategies. They will need to gain insights from data without sharing the actual data involved. One means by which they can do so is through the adoption of privacy-enhancing technologies (PETs) – cryptographic tools that allow data providers to share data for analysis in a modified form, and to pull insights from multiple data sources without disclosing private data.

As GovInsider has reported, inter-agency data sharing can support healthcare efforts and other whole-of-government projects.

In Estonia as long ago as 2015, the country's education and tax authorities used a PET known as secure multi-party computing to compare datasets in order to determine whether college students' take up of apprenticeships was linked to dropout rates. No actual data was disclosed to either authority.

The governments of Singapore and Estonia have recently taken steps to drive the adoption of such technologies in both the public and the private sectors.

Both countries are looking to tap the promise of data transfers to drive growth and greater convenience while maintaining high standards of data security in line with regulations, initiatives that necessarily involve PETs.

PET sandbox

Singapore's media and communications regulator, the Infocomm Media Development Authority (IMDA), and its data regulator, the Personal Data Protection Commission (PDPC), launched the country's first PET sandbox in July.

The sandbox is an experimental environment in which companies can work with PET suppliers on pilot projects. It aims to reduce the risks of traditional data sharing, open up opportunities for data collaboration between businesses, and unlock more data for use in training artificial intelligence platforms.

PDPC Deputy Commissioner Yeong Zee Kin told GovInsider: "PETs can support the essential elements of a digital economy – namely, the seamless transfer of data and the use of data to support innovation."

In implementing their pilot schemes, which will be supported by grants, companies can improve their understanding of which PETs to use to achieve their goals, understand their technical constraints, and get a better grip on regulatory compliance requirements.

A travel agency and a telecommunications company, for instance, could use secure multi-party computing to understand customers' travel preferences without disclosing any sensitive data, according to the IMDA.

Yeong said the PDPC, alongside the IMDA, will partner with sandbox participants throughout the programme's life "to identify the real-world regulatory and technical bounds of PETs and provide greater assurance to businesses to innovate with PETs while protecting consumer data". He said this would help the PDPC better understand what regulatory guidance might be helpful to map a path forward.

When it comes to the future of cross-border data collaboration, Yeong said PETs will be no panacea, as some cases might still require that data, rather than just insights, be shared. However, he said PETs will remain "an additional tool in the toolbox for regulators and compliance officers to make use of".

As part of an initiative known as the Global Partnership on Artificial Intelligence, the IMDA and the International Centre of Expertise of Montreal for the Advancement of Artificial Intelligence are collaborating on a project to demonstrate how PET can enable AI systems across multiple jurisdictions relating to such issues as climate action and health. PETs may be a key means of overcoming data barriers between commercial and government entities.

Singapore has also launched a Digital Trust Centre at Nanyang Technological University to deepen research on PETs and other trust technologies.

Estonia's 'Siri'

In the same week as IMDA's announcement, authorities in Estonia issued a procurement call for data professionals, both local and international, to develop and extend the use of PETs in the nation's "Siri of digital public services" – a system named Bürokratt, which aims to provide people with voice-activated public services.

Ott Velsberg, Estonia's Chief Digital Officer, told GovInsider that the country is planning to put together a government action plan on using PETs so that agencies can securely provide other agencies with access to sensitive datasets on the basis of consent.

Velsberg said Estonia's government information systems are decentralised, with each agency maintaining its own datasets. Estonian data regulations stipulate that data can be transferred between registries only for reasons stipulated in the law, and that any new uses would require changes in those rules.

He said that by using PETs such as homomorphic encryption – a form of data encryption which still allows for analysis – agencies can transfer insights and collaborate on projects without handling people's information at all. He also said PETs such as federated learning – a machine learning technique that trains algorithms across multiple decentralised repositories of data samples without exchanging them – can support agencies in processing data in their own systems and feeding those insights to develop centralised AI models.

Velsberg said that last December, Estonia had carried out pilot projects that generated synthetic data based on actual data. Synthetic data retains the overall characteristics of a dataset, but doesn't include any specific information on individuals. This could pave another way for making full use of government-held data.

Back to Table of Contents

Consent-based data sharing

Estonia's pilot schemes is taking place alongside efforts to provide individuals with more control over their data and give them rapid access to third-party services, which were informed by the understanding that for the government to offer people additional services, robust consent services were required.

"We need to respect different spheres of privacy, but at the same time we want to make maximum use of data," Velsberg told GovInsider.

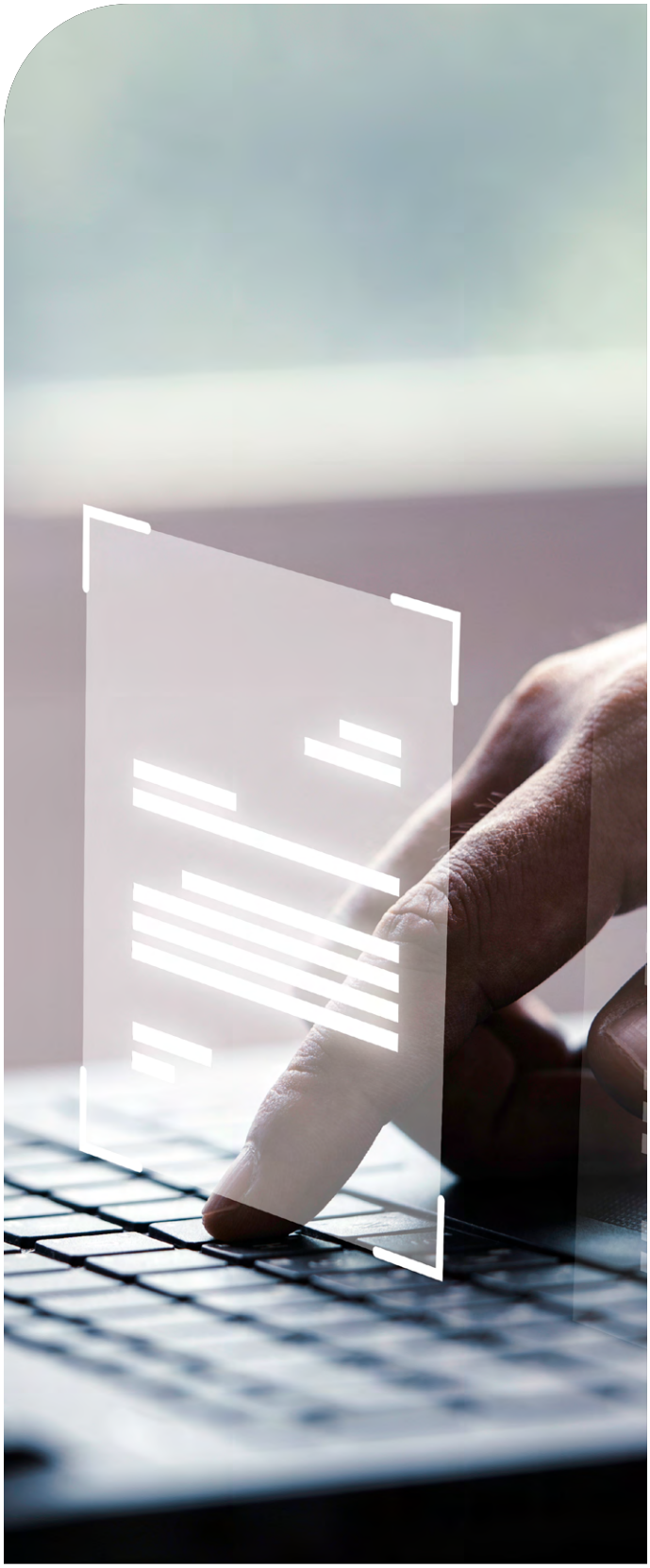
At the beginning of last year, Estonia's Information System Authority rolled out a digital consent service that allowed people to give permission to the state to share personal data with an external service provider. The service currently provides people with a choice to share solvency data from the country's Tax and Customs Board with digital lender Inbank. The bank can use the data to decide quickly whether a person can repay a loan in instalments, helping people avoid having to fill in numerous forms to apply for loans.

Velsberg said the service gives people the option of obtaining comparative offers, allowing them more choice, and even drives down loan interest rates. He said people also have access to a data tracker that gives them an overview of the data collected on them, who is using that data, and for what purpose.

He said more than 15,000 people had already used the service for loans, and that in the future, it might be expanded to facilitate the consent-based sharing of health data so that private sector entities could offer more personalised healthcare.

Velsberg said that PETs could in future help Estonia drive government-business data-sharing by enabling businesses to access only encrypted data or even synthetic data.

At the beginning of the year, a report in the Harvard Business Review said the data economy may soon be organised around gaining insights from consented data, and that sharing such insights would drive innovation, creating a secure data regime that simultaneously offers increased levels of convenience. As demonstrated by the trial schemes undertaken by Singapore and Estonia, government agencies and regulatory bodies are taking steps with PETs to shape the future of just such a data regime.



Back to Table of Contents

What's behind the global shift to data erasure?

By Blancco

Authorities worldwide, from Singapore's Government Technology Agency to a security-critical public agency in India, have shifted to erasing data with software to ensure their data management is watertight. Here's what you need to know about why and how.

Early this year, a well-known US investment bank agreed to pay US$60 million to settle a lawsuit over a personal data breach. Customers had argued that older servers that still contained customer data disappeared when the bank transferred them to an external vendor. The plaintiffs also accused the bank of failing to remove customer data before reselling two data centres to third parties.

Data leaks can come from anywhere, from poorly secured databases to hardware that is retired improperly. Yet the final step – disposing of data in a secure, verifiable manner – may be the most overlooked. But as the case above demonstrates, organisations need to pay as much attention to the data removal process as they do to maintaining high cybersecurity standards.

As governments accrue citizen data to provide more digital services, it is critical that every step of the data management process is accounted for to ensure that citizen data remains protected.

Strict security standards

Gone are the days when best practice was to wipe the contents of a hard drive with a magnetic pulse (degaussing) or physically destroy it using methods such as drilling or burning. Fredrik Forslund, Blancco's Vice President & General Manager International, earlier told GovInsider that although such physical methods may be more reassuring, they come laden with risks.

Degaussing has no effect on newer technology such as solid-state drives and certain types of hard disk drives. Physical destruction, such as by shredding, can also be risky, as many industrial shredders produce fragments much larger than the recommended width of 2mm, which can leave data vulnerable to recovery efforts.

NIST Special Publication 800-88 r1 is a US government document that lays out how an agency may securely sanitise data from storage media so all data is irretrievable. It includes the option of using software-based data erasure to combat keyboard-level data recovery attempts as well as laboratory-level recovery attempts that use advanced forensic techniques.

Agencies such as Singapore's Government Technology Agency, which is responsible for the delivery of the government's digital services, are increasingly including software erasure as a method to destroy data.

According to a Blancco press release, the company's software will be used on up to 100,000 computers available to Singapore's government agencies between 2022 and 2024. The PCs and laptops will come equipped with data erasure software, and providers will make site visits to erase outgoing hardware when devices reach end of life. Blancco's erasure software will also generate tamper-proof, digitally signed certificates of erasure that can verify all data has been removed.

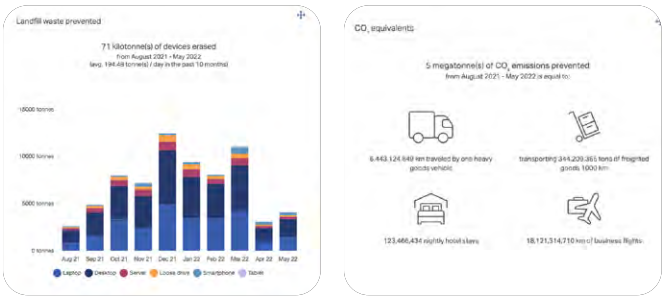
The certificates can also be hosted on a dedicated regional or local server, rather than on Blancco's cloud storage space, says Masayuki Morita, Vice President of APAC at Blancco Technology Group. This is in line with the increasing switch to storing sensitive data within geographical jurisdictions, rather than on distributed cloud platforms, that governments around the world are making.

Green goals

One benefit that comes with the shift to data erasure is that agencies can extend the life of their media storage devices – when data has been thoroughly erased, hardware can be reused. This can contribute to circular-economy goals and help agencies save money.

A Blancco survey of 596 public sector respondents globally found that organisations annually dispose of roughly one solid-state drive for every three employees, refreshing technology every three to four years, even while devices are still functional. This not only contributes to the growing problem of e-waste, but also leads to higher carbon emissions as manufacturers have to produce more hardware to replace outgoing technology. The manufacturing phase contributes to the largest percentage of carbon emissions, Morita says.

According to Morita, Blancco will soon be rolling out a sustainability dashboard that can track the potential carbon savings when agencies choose to extend the lifespan of their storage devices rather than refreshing technology with new devices.



Blancco's sustainability dashboard allows agencies to understand the quantity of carbon emissions and landfill waste avoided by securely erasing devices.

Image: Blancco

Once data is securely erased, agencies can either choose to reuse devices in-house, resell the devices, return leased devices, or donate the devices to charities. In Australia, Blancco is working with ICT service provider Ethan Indigenous to securely erase used government and enterprise laptops to enable indigenous young people to transition to economic independence through education and skills training for IT industry work. Blancco is also working with the non-profit Dariu Foundation in Vietnam to provide 70 rural schools and 2,000 disadvantaged children with free rentals of used desktops and laptops donated by businesses.

Streamlined data management

Finally, the shift to data erasure is also streamlining the process of managing data security for government employees. When agencies rely on physically destroying media storage devices, it can lead to inefficiencies. As devices move from hand to hand – from agency to external vendor – the chances of data leaks increase. This is especially true when an agency is moving thousands of devices, as the destruction of each device needs to be accounted for.

With data erasure, providers can perform immediate onsite sanitisation. Then, the system can automatically generate an audit trail to verify that each and every device has been erased. For peace of mind, agencies can also send a sample of devices to a digital forensic lab to confirm that data is no longer retrievable.

This is what a security-critical government agency in India did when it was shifting to software-based data erasure. After a specialty data forensics provider applied rigorous techniques to test drives erased with Blancco Drive Eraser, it concluded that the data had been completely eradicated and could not practically be recovered. This allowed the agency to securely transition to a workflow that helped it to improve both financial and environmental sustainability.

Morita also says that Blancco provides an application that can be hosted on an IT management platform – such as ServiceNow – so that government employees can track the erasure process smoothly and have full visibility over it.

When you run a marathon, the easiest part to overlook is cool-down exercises – but they're critical to relieving muscle soreness and bringing your body down to a state of rest. Secure data erasure is similarly vital: when government agencies incorporate the most up-to-date sanitisation processes into their policies and workflow, they can secure their data to the very end, improve their efficiency, and achieve their green goals.

Back to Table of Contents

Why data localisation may not be a panacea for data privacy woes in ASEAN

By Yogesh Hirdaramani

As concerns around data privacy increase, countries in Southeast Asia and beyond are increasingly turning to data localisation as a measure to protect personal data. But such measures should be applied with a risk-based approach, caution experts.

On October 1, a decree that requires international firms with services in Vietnam to store users' data within Vietnamese territory and set up local offices went into effect, reported Vietnam Express.

This new decree is an addition to Vietnam's existing Cybersecurity Law. It stipulates that data belonging to users, from account information to data about users' relationships, must be stored in Vietnam for at least 24 months. International firms must complete data storage requirements and set up local offices within 12 months of being asked to do so by the Ministry of Public Security.

In early September, US business groups representing technology companies such as Amazon, Google, and Meta said in a letter to Prime Minister Pham Minh Chinh that this law may affect investments and make it difficult for companies to assess the cost of doing business in the Southeast Asian country, reported Bloomberg.

Vu Tu Thanh, the Vietnam representative of the US-Asean Business Council, told Bloomberg that the new decree was drafted with the consideration of balancing economic interests and national security, and is more flexible than those in previous drafts.

An opinion piece on Nikkei Asia also highlighted that the decree may provide further leverage for the country's censorship requests to Big Tech.

Data localisation across the world

Vietnam's decree is part of a broader trend of data localisation in Southeast Asia and the world, which refers to the practice of:

1. requiring data to be collected, processed, and/or stored within a nation's borders, so that foreign actors cannot access them
2. requiring a copy of data to be kept in local servers or data centres, such that law enforcement agencies can access such data if found necessary
3. placing limits on the transfer of personal data across borders

The primary reasons for data localisation laws involve matters of national security. For instance, in June 2022, Chinese-owned social media app, TikTok, said that it planned to move the private data of American citizens to cloud servers in the US to allay privacy concerns, reported The New York Times. Keeping the data of American citizens within America may lower the risk of foreign governments accessing such data.

Storing data locally may also help local law enforcement agencies access data if necessary.

From 2013 to 2018, US law agencies were embroiled in a legal battle with Microsoft when the company refused to hand over data stored on a data centre in Ireland, according to TechCrunch. The case was eventually resolved with regulations that stipulated that companies must provide information properly requested by law enforcement regardless of location.

Countries may also pose limits on the transfer of personal data across borders if they assess that data protection regimes in other jurisdictions may not be adequate. For instance, the EU's General Data Protection Regulation (GDPR) ruled that personal data can only be transferred beyond the EU to external parties if the recipient country possesses a level of data protection equivalent to that of the EU.

In a journal article in the Asian Journal of International Law, Benjamin Wong from the National University of Singapore found low but significant levels of data localisation within ASEAN, with countries such as Philippines, Singapore, and Thailand possessing restrictions on the transfer of personal data across borders until certain standards of data protection are met.

Countries like Indonesia and Vietnam have regulations on processing and storing personal data within the nation's borders, as well as on hosting a local copy of data. East Asia Forum reported that Indonesian regulations require all public sector data to be managed, stored, and processed within the country.

Costs of data localisation

However, data localisation may come at a cost to economic growth and investments, as well as inhibit the performance of certain technologies.

First, data localisation imposes additional costs on companies, who may have to spend additional resources on setting up server rooms, data centres, and local offices, says Lim May-Ann, Emeritus Director of the Asia Cloud Computing Association. Larger countries may require more servers and infrastructure to properly serve the market, leading to high compliance costs to business.

If the cost is too high, companies may choose to pull out or suspend operations. In 2016, online payments company PayPal suspended operations in Turkey as a result of new regulations that required companies to fully localise their information systems within the country, reported TechCrunch.

Data localisation can also impede free trade and affect the regional economic development of ASEAN. Wong noted in his journal article that that such policies could obstruct businesses' access to foreign markets. This may run counter to the stated aims of the ASEAN Framework Agreement on Services, which aims to liberalise the trade in services, he argued. In fact, trade deals such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, which Vietnam is party to, includes pledges against data localisation, said Nikkei Asia.

Finally, data localisation may inhibit the performance and efficiency of current technologies like cloud computing and artificial intelligence. Cloud computing works most efficiently when data is able to flow across borders, and artificial intelligence works best when it has a diverse range of data sources to draw upon. Data localisation policies may inhibit both these functions.

A tool among a broader arsenal

Perhaps data localisation is best applied as one tool amongst many, with a risk-based approach in mind.

First, it is important to note that data localisation policies on their own may not necessarily improve the security of data. Data stored elsewhere on the servers of a cloud service provider may have higher cybersecurity controls than a local data centre, for instance. Restrictive data localisation policies may also be harder to enforce, notes Lim.

This is where a risk-based approach may prove useful, where each country sets its own risk level and decides how it would like to balance security and economic considerations.

A risk-based approach first requires countries to have strong data classification models, which can help identify which data is more sensitive than others, says Lim. For example, personally identifiable information may require more protections than non-personal data, and data directly related to national security may be best stored within national borders.

As it may not be feasible or cost-effective to store all data within one's country, a risk-based approach lets you "put as large a padlock as you want on the data that you think is most important," says Lim.

Back to Table of Contents

In Singapore and Malaysia, personal data protection laws regulate that organisations transferring data across borders have a responsibility to ensure that data continues to be protected at comparable levels to that of their home country. Singapore's Monetary Authority of Singapore has a technological risk management checklist, for one.

Other security best practices, such as the principle of least privileged access and zero trust systems, which requires portals to continuously verify one's identity through methods such as multi-factor authentication, can help secure data. Lim says that banks in the region, from Thailand to the Philippines, have been leading the front on the adoption of such practices.

Finally, the growth of privacy-enhancing technologies may also prove to reduce barriers to data transfers, as a recent GovInsider article noted, though Lim says that technology can only help insofar that people on the ground understand how to adopt and use such tech.

If ASEAN countries aligned on data protection standards, this would help encourage further economic integration and reduce barriers for the provision of services, much like the EU has done. However, Wong's article notes that ASEAN has a softer approach to regional regulations than the EU, and each ASEAN country will need to find its own path. As such, some restrictions on the transfer of data between countries may be inevitable.

Back to Table of Contents

The final frontier for cloud data security: secure erasure

By Blancco

As government agencies migrate data to the cloud, it is critical that they plan a clear data erasure strategy from the outset, say experts from Blancco.

The Covid-19 pandemic made cloud migration an inevitability for many governments. Moving to the cloud allowed public sector agencies to scale quickly, which became critical when the need for digital government services skyrocketed during the crisis.

The cloud is here to stay. It lets governments focus on their core jobs, allows them to access cost savings, and provides pre-built services for them to adopt. Yet, as delegates told the audience of AI x GOV 2022, agencies need to ensure data remains secure even as they seek to tap on the various benefits of the cloud.

As agencies put in place policies and regulations to ensure data remains secure on the cloud, it is critical that they consider their wider data security strategy and adopt the best practices for erasing data that is no longer needed.

Who's responsible for what?

Migrating data to the cloud can provide benefits in terms of scalability and flexibility, but agencies need to fully understand what they remain accountable for. That is, they will need to understand the role they may play in protecting data stored on the cloud and what responsibility resides with the cloud service provider. This is where the shared responsibility model can help shed some light.

"All the hardware lifecycle management and maintenance of hardware components are covered by the cloud service provider," Masayuki Morita, Vice President of APAC at Blancco Technology Group explains.

Cloud service providers – like Amazon Web Services – manage the security of the cloud, such as the physical security of the data centres as well as the security of the operating system. This frees agencies from the chore and costs of hardware maintenance, says Morita.

In turn, government agencies remain responsible for managing security within the cloud – that is, ensuring data remains secure. This can be done through means such as prudently managing access rights, keeping firewalls up to date, and erasing data that is no longer needed.

"Even though you use a public cloud system, you are not walking away from the accountability of protecting your customers' data. The data layer on top of the cloud infrastructure, that's what the user has to manage," Morita says.

What's the deal with data erasure?

Part and parcel of managing data storage is removing data that is no longer needed – storing unnecessary data can increase attack surfaces and vulnerability. Regulations like the EU's General Data Protection Regulation, Singapore's Personal Data Protection Act, and Japan's amended Personal Information Protection Act also require responsible data erasure management.

After all, data erasure is unavoidable – wherever information is stored, data erasure will eventually be needed, be it at the end of individual projects, when systems move to a different environment, or when regulations call for data removal. In some jurisdictions like the EU, Thailand, and South Korea, individuals also have the right to request for their personal data to be erased in certain cases.

When the need to erase data arrives, cloud users have the responsibility of erasing data so that it can no longer be restored, and producing auditable proof that erasure has occurred.

Cloud service providers need to provide the ability to do so, and third parties like data security firm Blancco Technology Group can come in to help agencies verify that erasure has taken place properly by generating tamper-proof reports and ensuring compliance with relevant regulations.

But how can governments plan for cloud data erasure from the beginning of their cloud journey? This is where encryption keys come into play.

Encryption keys – the key to data erasure

Unlike erasing data on hard drives or on on-premise servers, agencies rarely have access to the physical centres that host the public cloud, which may be distributed across the world. Physical erasure with methods such as shredding devices is not an option, and agencies have to rely on logical data erasure methods, explains Morita.

When data goes into the cloud, agencies need to encrypt such data with an encryption key. This ensures that only the user with access to the encryption key can decode the data – otherwise, the data will be unreadable. Establishing encryption keys from the get-go is a best practice for erasure management, Morita says.

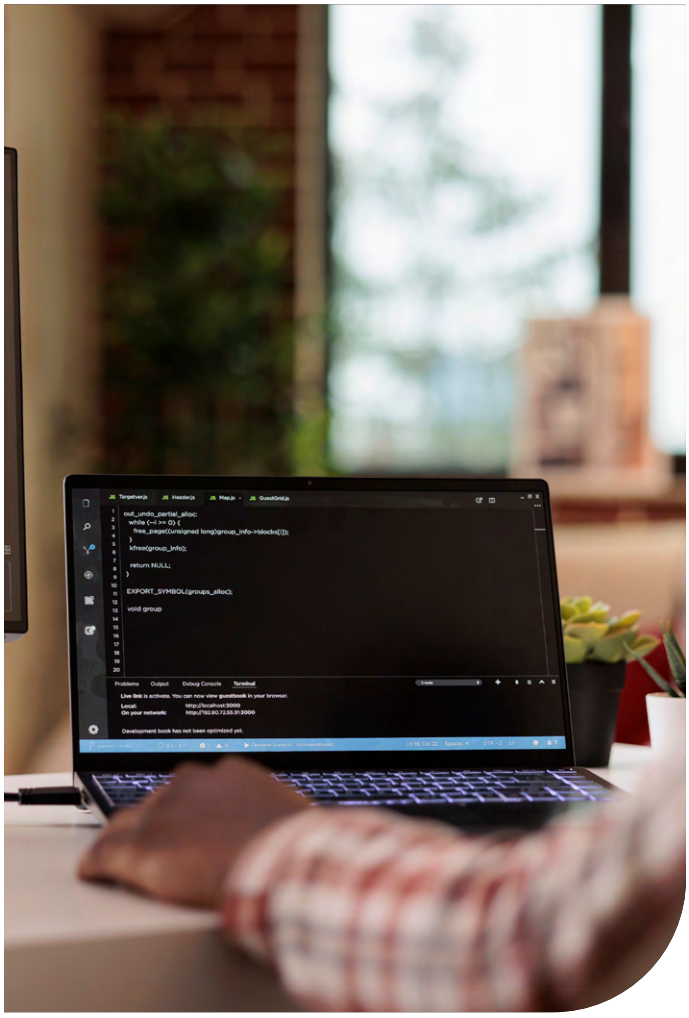
For example, the Japanese government's Information System Security Management and Assessment Program outlines that users must manage encryption keys and erase them to protect data in the cloud. When data is no longer needed, an agency simply needs to delete the encryption key and obtain verification that the key is successfully removed. This way, the original data will no longer be retrievable, explains Morita.

Accordingly, public cloud service providers are required to provide users with the tools that allow encryption key management and erasure, as well as information on how to use these tools. One example of this tool is the key management service offered by Amazon Web Services, which allows users to encrypt data and manage data encryption with an encryption key.

Amazon Web Services' storage services such as Amazon Simple Storage Service allows integration between Blancco's cloud erasure solution, Blancco Cloud Storage Eraser, and virtual environments. From the very beginning, agencies can create virtual spaces, or buckets, encrypted with an encryption key that users can create and upload themselves.

With this integration, Blancco facilitates erasure of all objects from the bucket, and the bucket itself. Blancco also produces tamper-proof erasure reports and an audit trail of the erasure process.

Similar to erasing data from hard drives, it is critical that agencies can be confident that their data erasure processes for data hosted on the cloud are reliable, verifiable, and auditable. Through Blancco's erasure solutions, any data hosted on the cloud can be thoroughly rendered inaccessible, and agencies can obtain certification to prove this.



Back to Table of Contents

GUIDE TO SECURE DATA DISPOSAL

GovInsider

IN PARTNERSHIP WITH

blancco