pwc

After Life

Critical infrastructure and the e-waste data security threat

What is the Problem?

Every year, Australian organisations dispose of thousands of tonnes of e-waste. Some is recycled, some is re-sold and some is shipped overseas - and a lot is not properly sanitised. The insecure disposal of e-waste, which remains a peripheral issue in the cyber security space, presents serious cyber and data security threats to Australian organisations and citizens. Notably, in the context of Australia's critical infrastructure regime, which has undergone significant reforms, there exists no explicit obligation for captured entities to securely dispose of e-waste. The data stored on these devices and their components may contain sensitive information related to an organisation's operations and intellectual property, as well as personally identifying information (PII). And if they end up in the hands of a malicious actor, the results could be catastrophic.

What is the Solution?

While there is no silver-bullet solution to prevent insecure e-waste disposal, there is a key policy lever that could be pulled to help drive uplift in this space. Therefore, this paper proposes the Security of Critical Infrastructure Act 2018 (SOCI Act) or its guidance should be amended to include explicit obligations for captured entities to securely dispose of e-waste when it becomes redundant. This would ultimately fill a significant gap in the legislation as it currently exists, ensure a truly holistic 'all-hazards' approach to cyber security risks and further bolster the cyber security of Australia's critical infrastructure entities.

It would also bring cyber security requirements of captured entities into line with the provisions Australian Government entities are required to adhere to under the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). More broadly, with the introduction of significant fines for serious or repeated privacy breaches now in force under the Privacy Act 1988 (Cth) (Privacy Act), captured entities must also be aware of this looming data security threat and take steps to ensure the secure disposal of e-waste to better protect PII.

Introduction

Reforms to Australia's critical infrastructure regime are central to ensuring operational security is at the forefront of maintaining the critical services and systems we all rely upon. And, while the reforms have been effective in driving security uplift in the 'here and now', a vital piece in the puzzle is missing - security threats posed by the afterlife of e-waste (electronic waste) and the data they retain.

Every year, Australian organisations dispose of thousands of tonnes of e-waste. Some is recycled, some is re-sold and, while an accurate measure is impossible to determine, based on anecdotal evidence much of this e-waste is not properly sanitised. This e-waste and its insecure disposal, to which little attention has been paid, presents serious cyber and data security threats to Australian organisations. The data stored on these devices and their components may contain sensitive information related to an organisation's operations, intellectual property and highly sensitive personally identifying information (PII). And if these devices end up in the hands of a malicious actor, there is the potential for significant cyber and data breaches.

In the context of critical infrastructure, where the security stakes are high, the looming spectre of e-waste data security vulnerabilities is an issue that deserves everyone's attention. Put simply, in taking an all-hazards approach to risk management, are critical infrastructure entities ensuring e-waste security threats are appropriately mitigated?

This paper examines what e-waste is and the potential risks it poses to data security. This 'forgotten' threat vector is explored in the context of Australia's critical infrastructure regime, which has undergone significant reforms over the past several years, and as it relates to the Privacy Act, which has had an overhaul of its fines regime and remains under review. It also presents practical and pragmatic recommendations for critical infrastructure entities to help ensure that, as part of their security risk management processes, secure disposal of e-waste is a key consideration.

Implementing effective cybersecurity controls – especially against a backdrop of complex and dynamic legislative and regulatory regimes – can be difficult to navigate. And in an environment that tends to focus on the present, it is easy to tick, flick and forget end-of-life e-waste processes. But the stark reality is that critical infrastructure entities without secure end-of-life e-waste procedures could literally be handing cyber criminals the keys to their castle.

What is e-waste?

As defined by The Global E-waste Statistics Partnership, e-waste is: “All items of electrical and electronic equipment and its parts that have been discarded by its owner as waste without the intent of re-use. E-waste is also referred to as WEEE (Waste Electrical and Electronic Equipment), electronic waste or e-scrap in different regions and under different circumstances in the world. It includes a wide range of products – almost any household or business item with circuitry or electrical components with power or battery supply”.[1]

The most recent figures available indicate that in Australia and New Zealand about 650 kilotons of e-waste is produced annually and, of this, only 59 kilotons are formally collected - about 10 per cent.[2]

While the detrimental environmental implications of the e-waste tsunami have been widely explored, the serious cyber security risks associated with data retained on discarded devices have not. This is an area that needs urgent attention given predicted future trends - it is estimated by 2030 the volume of global e-waste will exceed 70 million tonnes[3] per year. This increase is largely due to the rapid proliferation and turnover of Internet of Things (IoT) devices. It is estimated by 2030 there will be more than 25 billion IoT devices globally[4] - and these devices store vast amounts of valuable data.

Billions and billions: IoT proliferation

The Internet of Things (IoT) comprises billions of physical internet-connected devices around the world that collect and share data. IoT comprises everything from smart watches and home refrigerators right through to drones and planes. The use of sensors means IoT devices can ‘communicate’ real-time data without the need for human operation, creating autonomous and ubiquitous systems that meld the physical and digital worlds.[5] IoT systems are central to the operations of modern critical infrastructures, which rely on a vast array of data-producing and storing sensors and control devices to ensure autonomous, efficient and stable supply of critical services. Given the rapid rate of IoT proliferation and the vast volumes of data-storing components these devices comprise, there are a myriad of cyber and data security implications that could arise due to unsecure IoT disposal.

1 Global E-waste Statistics Partnership
2 Country Sheets: Australia and New Zealand
3 E-waste surges in 2021 as world sends goldmine to landfill - ABC News
4 Internet of Things statistics for 2022 - Taking Things Apart
5 What is the IoT? Everything you need to know about the Internet of Things right now | ZDNET

Testing the theory - An experiment

Little formal research has been conducted into investigating the types of data left on redundant devices. However, the research that has been done paints a grim picture. Furthermore, there is significant anecdotal evidence, as indicated by a small experiment undertaken for this paper and discussions with a secure destruction expert, which indicate this problem is widespread.

In March 2023, for the purposes of this paper, two devices were bought from a popular second-hand retailer in the ACT. The mobile phone and tablet were purchased for less than $50, but analysis indicated the data stored on these data could be worth a significant sum if sold illegally. Using basic analysis, 65 pieces of PII were recovered from the phone, including home address, personal documents and photographs. The tablet, from which corporate stickers had not been removed, was particularly concerning. It contained a note with credentials for access to a database which could enable access to up to 20 million sensitive PII records.

Globally, we could find only two studies in which similar analysis had been conducted.

In 2019, a US-based cyber professional bought 85 used devices online for US$650 to see what information could be retrieved from them. More than 366,300 files were recovered, including images and documents and PII like social security numbers, credit card and passport numbers. In all, the data of just two of the devices had been properly wiped.[6]

In a similar experiment, University of Hertfordshire researchers bought 200 USB memory sticks (100 in the US, 100 in the UK) from online sellers, secondhand shops and traditional auctions. They found two-thirds of USB drives still contained remnant data from previous users, including a wide range of intimate, private and sensitive files like nude photos, business documents, ID scans, job applications, wage slips, tax statements and medical documents.[7]

6 Exfiltrating Remaining Private Information from Donated Devices | Rapid7 Blog
7 Two-thirds of secondhand USB drives still contain previous owners' data: study - Comparitech

What is secure disposal?

Secure disposal of e-waste is complex - it is about much more than hard drives. And when it comes to devices holding sensitive information, professional disposal by a National Association for Information Destruction AAA (NAID AAA) certified provider should be considered.

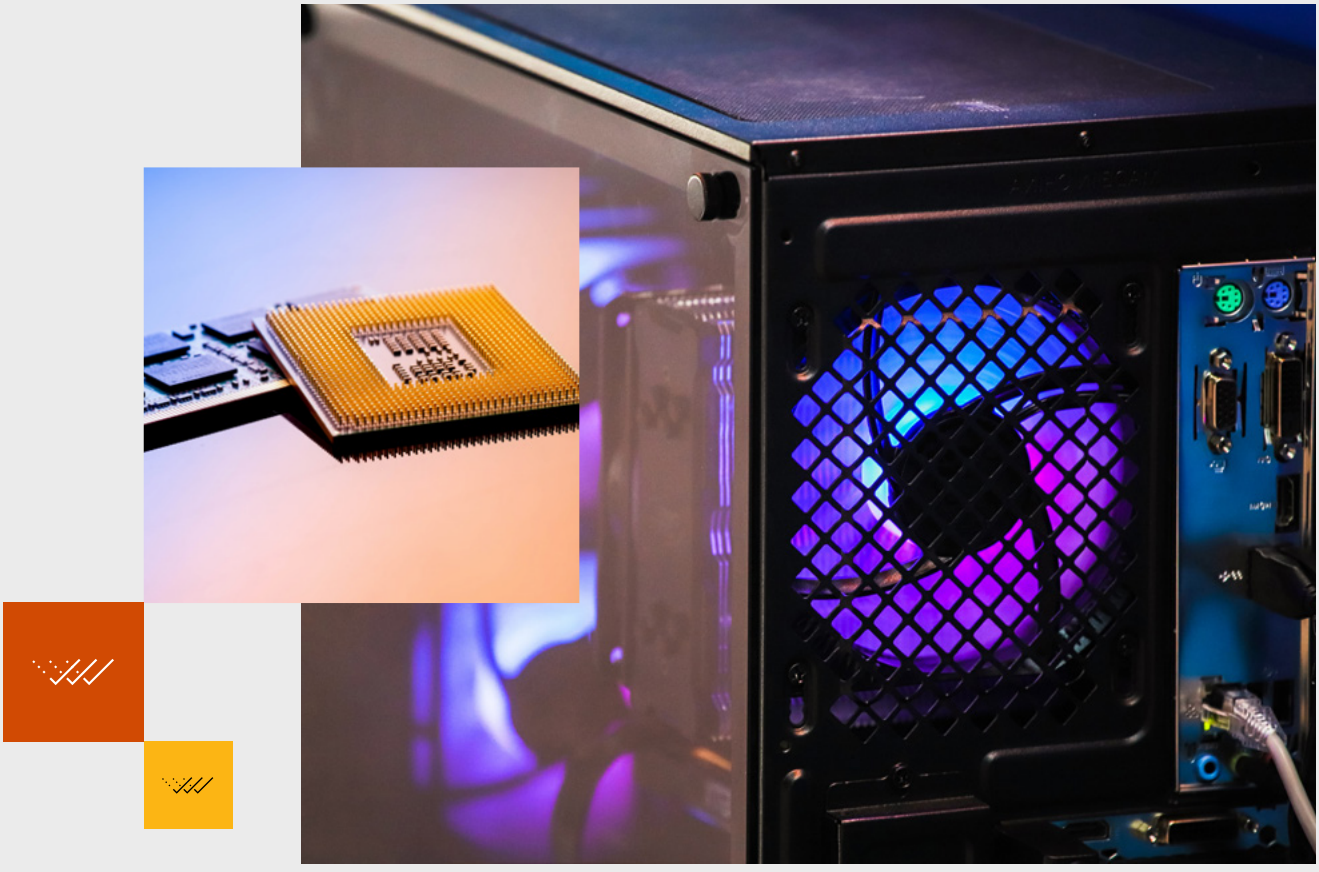
One of the key processes that needs to be carried out is degaussing of magnetic storage devices, like hard drives. Degaussing magnetic media using a coercive magnetic force changes its properties, which results in data being permanently corrupted and rendered unrecoverable.[8]

However, coercivity is variable between magnetic media types, brands and models, meaning attention must be paid to the strength of the magnetic field that is applied. If it is not strong enough, data may be retained on a device and, therefore, recoverable.[9]

If there is an intention to re-sell used devices then organisations should ensure they are properly wiped. Again, requirements vary from device to device. As part of this process attention must be paid to the numerous media storage devices like hard drives, flash memory, solid state drives and USB flash drives.[10]

Furthermore, any identifying marks or stickers on the device should be removed.

And finally, for devices holding extremely sensitive information, consideration should be given to complete physical destruction of all components. Ultimately, this involves the devices being shredded into 3-6mm pieces by an industrial-grade shredding machine.



8 https://www.cyber.gov.au/sites/default/files/2021-12/14.%20ISM%20-%20Guidelines%20for%20Media%20%28December%202021%29.pdf
9 Degausser | Cyber.gov.au
10 What is a storage medium (storage media)?

PSPF and ISM obligations

The Australian Government's information security framework is captured in two documents - Protective Security Policy Framework (PSPF), which is administered by the Attorney-General's Department, and the Information Security Manual (ISM), which is administered by the Australian Signals Directorate (ASD).

The Protective Security Policy Framework (PSPF) sets out the requirements Australian Government entities must abide by in relation to protecting information and assets. One of its four pillars relates to information security. According to the PSPF, "entities must ensure security classified information is stored, transferred, and disposed of appropriately".[11] The PSPF guidelines mandate that procedures and processes contained within the ISM should be followed for the purposes of secure disposal.[12]

The ISM contains strict and prescriptive conditions for the disposal of redundant devices storing sensitive information. It states that: "Before ICT equipment can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed or declassified ICT equipment still presents a security risk, albeit very minor, an appropriate authority needs to formally authorise its release into the public domain. Furthermore, as part of disposal processes, removing labels and markings indicating the owner, sensitivity, classification or any other marking that can associate ICT equipment with its prior use will ensure it does not draw undue attention following its disposal".[13]

The ISM outlines that, for secure destruction of materials below TOP SECRET classification, a National Association for Information Destruction AAA (NAID AAA) certified destruction service can be used.[14] NAID AAA certified destruction facilities ensure stringent protocols are in place to ensure the security of confidential material throughout all stages of the destruction process such as handling, transporting, storing materials prior to destruction and destroying and disposing of materials responsibly.[15] It also notes that the destruction of devices storing highly sensitive data should be supervised by at least two personnel, who also sign a destruction certificate afterwards.[16]

11 Policy 8: Sensitive and classified information
12 https://www.protectivesecurity.gov.au/system/files/2023-01/pspf-policy-08-sensitive-and-classified-information.pdf
13 Information Security Manual (ISM) | Cyber.gov.au, P71
14 Ibid 13, P81
15 NAID AAA Certification in Canberra | Shred-X
16 Ibid 13, P80

E-waste disposal: WV Technologies

According to Kurt Gruber, there are dozens of digital components that contain data and need to be sanitised or destroyed to ensure the effective secure disposal of e-waste. Mr Gruber and his team at Canberra-based secure ICT asset disposal company WV Technologies have been in the industry for decades and the company holds a NAID AAA certification with PSPF endorsement.

Over the years, the WV Technologies team has been shocked at the sensitive data they have encountered. They have intercepted troves of highly sensitive information held on the bulk lots of computers and networking equipment (like switches and phones) bought from used IT resellers, auctions and online sales of used electronics - devices anyone can freely buy. This includes comprehensive personal details gathered by major retailers, health and child safety records, the alarm codes for every outlet of a major retailer, scanned driver licenses and credit card details retained by a storage company, as well as medical and personal records of government employees. And this is just the tip of the iceberg.

Mr Gruber said many organisations opted to utilise cheaper, non-accredited IT asset disposal companies, undertake sanitisation in-house and give-away or on-sell old devices without undertaking effective sanitisation. Many of these devices ultimately end up in the public marketplace with potential for them to be acquired by malicious actors.

What is ‘critical infrastructure’?

‘Critical infrastructures’ are the vital systems and services that underpin our way of life. As defined by the Federal Government, they are the “physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia’s ability to conduct national defence and ensure national security”.[17]

Over the past several years, the laws governing Australia’s critical infrastructure have undergone significant reform, driving security uplift across our nation’s critical infrastructure sectors, the number of which have been expanded from four to 11.

Captured sectors provide essential services to Australians and are vital to ensuring our national security and way of life.

For the purposes of critical infrastructure legislation and its practical application a holistic interpretation of ‘security’ must be applied, capturing cyber security, physical security, personnel security and supply chain security. Such an approach is essential to developing an ‘all-hazards’ view to securing critical infrastructure and helps identify gaps and weaknesses within organisational systems.

Critical Infrastructure sectors

- Energy
- Communications
- Data storage or processing
- Financial services and markets
- Water and sewerage
- Health care and medical
- Higher education and research
- Food and grocery
- Transport
- Space technology
- Defence industry[18]

17 Critical Infrastructure Resilience Strategy: Plan
18 Critical Infrastructure Sectors

Critical Infrastructure and Cyber Security

Under the new regime, assets from across 13 designated asset classes are required to fulfill Critical Infrastructure Risk Management Program (CIRMP) obligations and must comply with one of five mandated cyber security standards or a combination of several. Under the legislation, a cyber and information security hazard "includes where a person, whether authorised or not, improperly accesses or misuses information or computer systems about or related to the asset, or where such person by use of a computer system obtains unauthorised control of or access to any function which may impair the proper functioning of the asset".[19]

Under CIRMP rules, impacted entities are required to: maintain a process or system to minimise or eliminate material risk a cyber and information security hazard that could have a relevant impact on the asset; mitigate the relevant impact of a cyber and information security hazard on the asset; and minimise any material risk of a cyber hazard occurring.[20]

Furthermore, Section 5 of the SOCI Act defines what information and data is to be treated as 'protected information'.

This category of information should form the focus for the CIRMP rules and be prioritised for protection over the lifecycle of data. Consideration should be given to expanding the guidance on the treatment of this information - especially its unauthorised disclosure - to include destruction.

While the mandated standards for CIRMP rules are useful in managing cyber threats, understanding risk vectors and implementing mitigations, none include guidance regarding the secure disposal of redundant devices. Furthermore, within the CIRMP there is no explicit obligation for secure disposal of the e-waste of captured assets, which has the potential to expose such entities to cyber threats emanating from unsanitised devices.

Ultimately, this means there is no obligation to ensure the sanitary disposal of e-waste as it relates to captured critical infrastructure assets - assets that if compromised by a cyber attack, could have significant ramifications for Australia's national security and economic prosperity, and potentially even endanger life.

The 13 CIRMP asset classes:

- critical broadcasting asset
- critical domain name system
- critical data storage or processing asset
- critical electricity asset
- critical energy market operator asset
- critical gas asset
- designated hospital
- critical food and grocery asset
- critical freight infrastructure asset
- critical freight services asset
- critical liquid fuel asset
- critical financial market infrastructure asset
- critical water asset.[21]

The five security standards are:

- ISO 27001:2015
- Essential Eight Maturity Model – meet maturity level one
- Framework for Improving Critical Infrastructure Cybersecurity
- Cybersecurity Capability Maturity Model – meet Maturity Indicator Level 1
- The 2020-21 AESCSF Framework Core – meet Security Profile 1.[22]

19 Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022
20 Ibid 19
21 CISC: Regulatory obligations
22 Ibid 21

Beyond critical infrastructure - The wider economy

Over the past several years there has been significant cyber-related legislative and regulatory focus in Australia and this trend is set to continue. This year will see the release of the 2023-30 Australian Cyber Security Strategy, which will focus on broadening the SOCI Act and hardening government systems, and ongoing consultation into Privacy Act reform, aimed at ensuring Australia's privacy laws are fit for the digital age.

In the wake of several high-profile cyber attacks in Australia in 2022, the Federal Government took swift action, overhauling the Privacy Act's fine regime for "serious or repeated privacy breaches". The new regime applies to any organisations captured by the Privacy Act - broadly speaking organisations with annual turnover of more than $3 million - which comprise a large cross-section of the economy.

The Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Enforcement Act) came into effect in December 2022, increasing maximum penalties that can be applied under the Privacy Act for serious or repeated privacy breaches from $2.22 million to whichever is the greater of:

- $50 million;
- three times the value of any benefit obtained through the misuse of information; or
- 30 percent of a company's adjusted turnover in the relevant period.[23]

It also provides the Office of the Australian Information Commissioner (OAIC), Australia's privacy regulator, with greater powers to resolve privacy breaches and strengthens the Notifiable Data Breaches scheme to ensure the OAIC has comprehensive knowledge and understanding of information compromised in a breach, so risk of harm to individuals can be better assessed.[24]

Australian Privacy Principle (APP) 11.2, states that entities must "take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs". Furthermore, the OAIC's Guide to Securing Personal Information (the Guide) notes that "destroying or permanently de-identifying personal information that you no longer need is an important risk mitigation strategy".[25] While the Guide does present a series of useful questions for organisations to consider in dealing with destroying data (including that contained on redundant devices), it does not present a binding or prescriptive guidance for organisations to follow, especially smaller organisations.

Given the looming significant changes to the Privacy Act - and the significant fines now in place - secure disposal of e-waste should also be a primary concern for organisations not deemed critical infrastructure but captured by the Privacy Act. In particular, this should capture the attention of organisations holding significant amounts of PII and sensitive information like retailers, professional services providers and not-for-profits. For such organisations, data security should be front of mind and include provisions for the sanitisation or secure disposal of e-waste.

23 Shifting sands: Preparing for the inevitable reform of Australian privacy and cyber security regulation
24 Ibid 23
25 Guide to securing personal information - Home

Conclusion

As the systems and functions society relies upon become ever-more digitised, serious consideration must be given to how the vast amounts of e-waste, and the valuable data they hold, is securely disposed of.

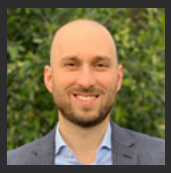
There is no doubt that amid an increasingly complex regulatory and legislative cyber security backdrop, organisations are making big changes to the way they protect data during its lifecycle. But, as this report has explored, there are significant risks posed by unsanitised e-waste and, anecdotally, there is clear evidence poor sanitisation and destruction practices are widespread. Hence, there is an urgent need to, as a first step, ensure that Australia's critical infrastructure entities are required to securely dispose of redundant devices.

Furthermore, with the introduction of significant penalties for "serious or repeated" breaches of the Privacy Act, this is an issue that requires attention more broadly across the economy.

To this end, this paper proposes two key recommendations:

- Consideration should be given to amending the SOCI Act to ensure secure disposal of e-waste is an obligation under CIRMP rules. This would bring industry into line with the obligations Federal Government departments and agencies are required to adhere to in relation to secure disposal (PSPF and ISM) and help further bolster security of Australia's critical infrastructure. The introduction of such obligations would be reported as part of an organisation's CIRMP, which is subject to board attestation, supporting a 'double-lock' mechanism in implementation and accurate reporting.
- The OAIC could provide specific guidance or memo beyond the existing Guide in relation to the secure disposal of redundant devices for organisations captured by the Privacy Act. This could include key steps that organisations should undertake to ensure their e-waste is securely sanitised or destroyed. Such guidance would be of particular assistance to small and medium enterprises, which have more limited resources and expertise to support secure disposal practices.

Contact us



Robert Di Pietro
Cybersecurity & Digital Trust Leader
+61 418 533 346
robert.di.pietro@pwc.com

Anne-Louise Brown,
Senior Manager,
Cybersecurity & Digital Trust
+61 406 987 050
anne-louise.brown@pwc.com

Explore more

pwc.com.au

D0485029