UNSW SYDNEY

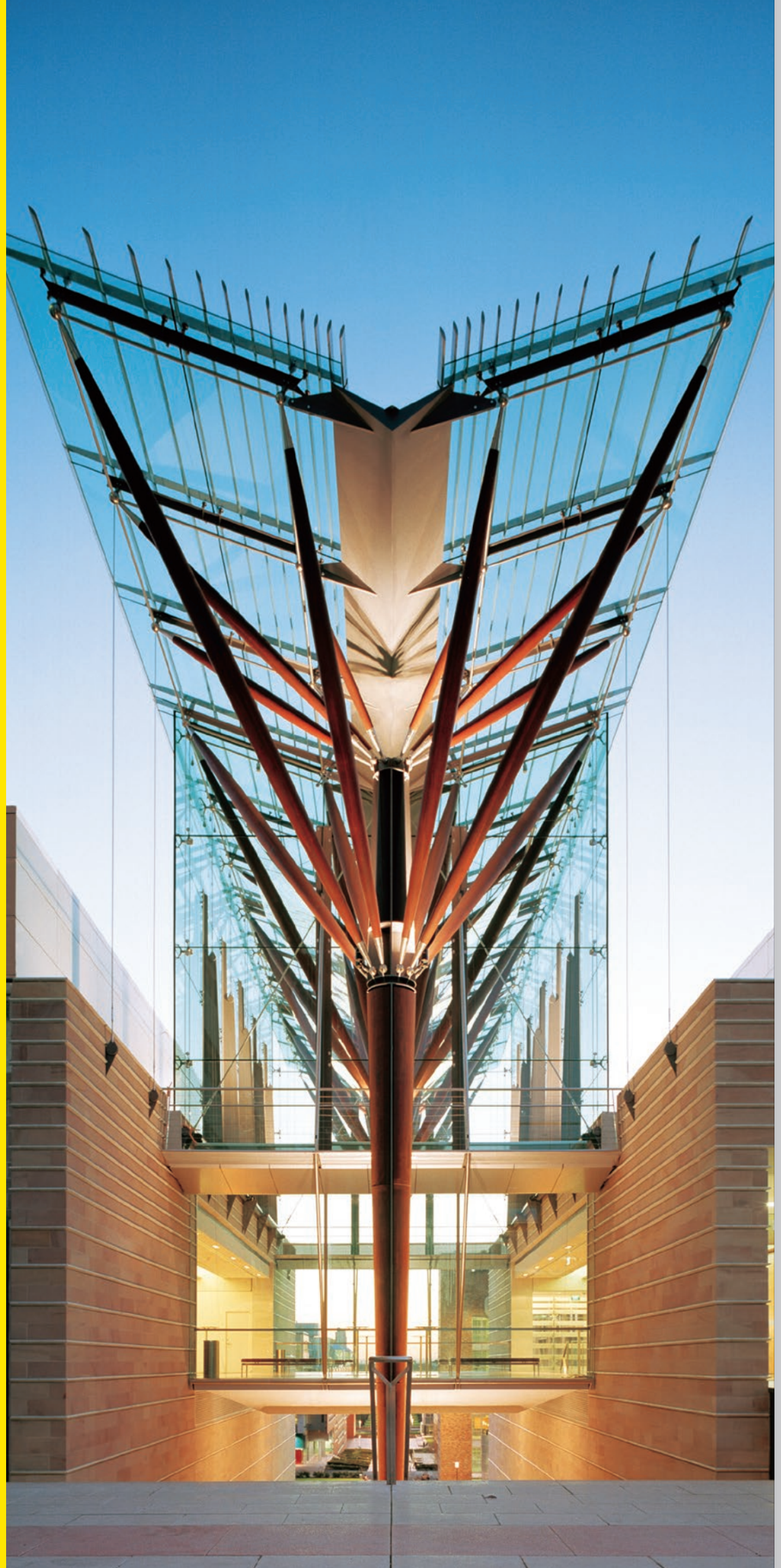
Considerations for Managing Cyber Threats to the Consumer Data Standards:

A Report to the Data Standards Chair

Lyria Bennett Moses, UNSW Sydney
Richard Buckland, UNSW Sydney
Rahat Masood, UNSW Sydney
Benjamin Turnbull, UNSW Canberra

June 2022

Contents



FOR PUBLIC RELEASE

FOR PUBLIC RELEASE

Purpose Statement

About this report

The purpose of this Report is to inform the Data Standards Chair (**Chair**) in relation to their obligation in regards to the Threat Modelling component of security risk management for the Consumer Data Standards (**Data Standards**), with a particular focus upon cybersecurity risks. It explains why a Threat Modelling capability for the Data Standards is necessary and how it ought to be designed. It is not itself a Threat Modelling activity, and therefore does not identify all Threats or explain how they might be mitigated. The Report is based on an analysis of the current cyber-security threat-landscape, in the context of the Consumer Data Right (**CDR**), and with reference to applicable international standards.

This Report was written in relation to a Statement of Requirements. Work on this Report took place over the period 27 May 2022 to 30 June 2022, with changes made during consultation with the Department of the Treasury up to 31 August 2022. The project scope did not include consultation with stakeholders; we have, however, made recommendations in relation to consultation going forward

Objectives

The objective of this Report is to provide an initial view on Threat Modelling for the Data Standards, ensuring that the approach recommended is fit-for-purpose and maintainable and meets the needs of the Data Standards Chair.

This Report provides the Chair with:

1. an analysis of relevant Threat and Attacker modelling methodologies, and relevant international standards, concluding with a recommended approach for Threat Modelling;
2. a description of the current, and emerging, state of Threat Actors, which could target the Data Standards; and
3. a set of recommendations to the Chair for how to maintain a Threat Modelling capability for Data Standards development.

Disclaimer

This Report is provided solely for the benefit of the Data Standards Chair, who is an Official of the Department of the Treasury. It does not constitute legal advice as to application of laws and regulatory instruments to particular fact scenarios or in particular contexts and should not be used as such. Formal legal advice should be sought in particular matters. While information in this Report has been formulated with due care, the University of New South Wales (**UNSW**) and its subcontractors disclaim and exclude liability to any person, other than the Data Standards Chair and the Commonwealth Treasury, for use of information in this Report.

Citation

This Report should be cited as Lyria Bennett Moses, Richard Buckland, Rahat Masood, Benjamin Turnbull, *Considerations for managing cyber threats to the Consumer Data Standards: A Report to the Data Standards Chair* (UNSW, 2022).

Section 3 was written under subcontract with Willis Towers Watson and was co-authored by Benjamin Di Marco and Rob Wiggan with assistance from Olivija Radinovic, Timothy Jones, Lyria Bennett Moses and Richard Buckland.

Executive Summary

Cybersecurity is a matter of national concern. The Australian Institute of Criminology estimates that the annual cost of cybercrime to individual consumers in Australia in 2019 was $3.5 billion, with 15% annual growth. This cost includes approximately $1.9b directly lost by victims, $600m dealing with the consequences of victimisation, and $1.4b spent on prevention costs.[1] More broadly, the security of networked digital systems from a broad range of Threats including but extending beyond cybercriminals – including those related to hostile nation states, mistakes and disasters, and potential actions by hacktivists – is essential in the modern digital economy.

The broader Threat environment impacts on Threats that specifically affect the Consumer Data Right (**CDR**) ecosystem, a network of CDR data, entities in designated sectors that hold CDR data (**Data Holders**), Accredited Data Recipients (**ADRs**), Trusted Advisers, consumers, and third-party supply chain agents. There are a range of Threat sources, including Threats from nation states, sophisticated criminals, and participants in the CDR ecosystem as well as through supply chains. Some of these stem from malicious Actors while others arise from mistakes and incompetence. The reputation of the CDR and consumer confidence and willingness to use it are key government assets. The management of Threats to the CDR, by the Chair and government, influences consumer perception of its trustworthiness, especially in the context of growing public awareness of the importance of digital privacy and good cybersecurity practices. Effective, and visible, security risk management would have a positive impact on protecting the reputation of the CDR, particularly when a cyber security event occurs.

This Report, addressed to the Data Standards Chair (**Chair**), provides guidance on the role that a consideration of Threats should play in the exercise of their statutory powers and functions. By describing the Threat landscape and drawing on examples, it highlights the importance of the Chair understanding Threats impacting on the CDR. The Report also outlines how that Threat Modelling ought to be conducted, both in terms of methodology and in terms of timing and approach. In addition, it identifies some other considerations adjacent to Threat Modelling to assist the Chair in fulfilling their obligations in relation to the role of Data Standards in enhancing security of the CDR ecosystem.

The core recommendation of this Report is the importance of the Chair adopting and continuously iterating a methodology to discover, enumerate, and evaluate Threats. Understanding who and what might threaten the security of the data at the centre of the CDR ecosystem and how attacks might occur will position the Chair to weigh foreseeable risks that might arise out of or be mitigated by the exercise of their powers and functions. Understanding and countering Threats to data in the CDR ecosystem, constructed and protected through Data Standards, will enhance the security of the national digital economy. Trustworthy Data Standards, written with an understanding of the Threat environment in which they operate, will give consumers and participants confidence that their participation will not come at the expense of their security and privacy. Data Standards that address Threats throughout the entire data lifecycle will limit the ability of Attackers to exploit the "weakest link" beyond the scope of current Data Standards. Data Standards that account for and adapt to changes in the increasing Threat environment can protect the digital lives and interactions of 26 million Australians into the future.

Recommendations to the Data Standards Chair

1. **Critical - Conduct Threat Modelling.**
Threat Modelling for the CDR should focus on Threats to consumer data over the entire data lifecycle. An initial formal Threat Modelling activity should be carried out as soon as practicable and should be undertaken by an independent party. The results of this should be openly reported (with appropriate publication delays for rectification of any critical vulnerabilities identified).

2. **Essential – Continuous ongoing Threat Modelling.**
Ongoing Threat Modelling should be conducted as part of a Risk Management Framework (**RMF**). A formal, independent, openly reported Threat Modelling activity of the form set out in Recommendation 1 should be conducted periodically over the life of the CDR, supplemented by a continuous ongoing internal capability. This formal Threat Modelling should be conducted at least every two years and more frequently as warranted, for example when there are significant changes in the Threat environment or CDR scope. We recognise this will mean, in practice, that formal Threat Modelling is more frequent than every two years. Furthermore, formal and openly reported Threat Modelling should be conducted during the planning phase before implementing any major changes in CDR scope or functionality,[2] and as part of any post-incident response.

3. **Recommended - Within 1 year, establish a Data Standards Cybersecurity Expert Advisory Panel.**
A Data Standards Cybersecurity Expert Advisory Panel should be established to provide advice and support to the Chair as they require on matters of cybersecurity, including identification and analysis of Threats relevant to Chair's obligations with respect to Data Standards. The panel would provide expert advice and support in scoping and reviewing cybersecurity reports and additional governance activities as appropriate (for example penetration testing and cyber health checks). It would also give advice to the Chair on request and support the Chair to be responsive to new Threats to the Data Standards as they emerge. The panel would be constituted with experts drawn from: relevant governance bodies (including the Australian Competition and Consumer Commission (**ACCC**) and the Office of the Australian Information Commissioner (**OAIC**)), academia (with expertise in fields such as cybersecurity, risk, incident response, cybersecurity training and communication, psychology and behaviour), relevant professions in industry, cyber mature CDR participants, and equivalent bodies overseas.

4. **Recommended - Collaborate openly with other stakeholders on an ongoing basis.**
Due to the wide scope of Threats to the CDR ecosystem as a whole, identifying and assessing Threats will require formal and informal mechanisms for maximising communication and collaboration with all bodies with responsibility for different aspects of CDR governance (including the ACCC and the OAIC). We recommend increasing communication flows, reducing silo barriers and fostering genuine partnership to ensure security risk management, including Threat Modelling, works holistically. The outcomes of Threat Modelling, including reports, reviews and security mechanisms put in place subsequently, should be done openly and shared with stakeholders. Such collaboration among stakeholders aligns with the work already being done in partnership with international organisations such as the OpenID Foundation.

5. **Essential - In the context of Recommendations 1 and 2, conduct Threat Modelling with a wide lens.**
The Chair should, in doing Threat Modelling, use a wide lens to capture all Threats to the CDR ecosystem rather than focussing on Threats pertaining specifically to Data Standards. The kinds of Threats that should be considered include:

    a. Threats throughout the entire CDR data lifecycle, including (1) Threats relating to the transfer of data to Trusted Advisers, and (2) Threats leading to re-identification of data that has been through a de-identification process in accordance with CDR Rule 1.17;

    b. Threats of consumer mistakes and misunderstandings;

    c. Threat Actors using social engineering; and

    d. Threats to ongoing development capability to support internal security functions, including loss of key employees or contractors.

6. **Critical – Establish a capability for Threat assessment and modelling in the Data Standards Body (DSB).**
This capability should be mature and sufficiently resourced to conduct the continuous and ongoing Threat Modelling activity outlined in Recommendation 2. As noted in Recommendation 5, Threat Modelling should consider and assess Threats which could arise from insufficient resources to support internal security functions and from the loss of key employees or contractors. In addition to including these in the Threat Modelling activity, such resources are essential to support the Threat Modelling activity itself. In particular, resourcing is required to maintain a minimum acceptable level of data security functionality and the ability to conduct ongoing Threat Modelling in accordance with our recommendations.

7. **Critical – Put in place a Data Standards Safety System.**
The Chair needs to plan how to respond to different situations in advance of an attack or crisis. This might include mechanisms to iterate Data Standards quickly in response to an identified vulnerability. Some form of Data Standards Safety System is needed to set out processes and systems to respond to critical situations in appropriate timeframes. It would also incorporate regular testing and emergency drills for training and evaluation of processes and system effectiveness. Ideally, CDR participants would (1) exchange Threat information with the Chair and other CDR participants, (2) do so in a standardised way; and (3) **coordinate** their emergency plans and conduct joint tabletop practice exercises to rehearse responses to scenarios. The Chair may wish to encourage these actions through Data Standards and guidance.

8. **Recommended - Conduct a structured approach to Threat Modelling that aligns with government risk management policies, using a synthesis of the OWASP-TMP Threat Modelling methodology and the STRIDE Threat classification framework.**
The OWASP-TMP methodology is contained in its "Threat Modeling Process".[3] STRIDE is an acronym referring to six categories of Threat, and provides a structure to identify Threats using a goal-based approach.[4] As explained in Section 4 of this Report, this recommendation is consistent with government risk management policies, including the Information Security Manual (**ISM**), in particular, Security Control ISM-1238; Rev 4.

Commendation: Openness.
The Data Standards development process is an exemplary demonstration of best practice in openness and transparency. All community and participant comments, submissions, and versions are published publicly on GitHub with full logs and version control. This demonstrable commitment to openness forestalls accusations of secrecy and evasiveness in times of post incident stress and media attention, supporting public confidence, and as such is a valuable asset to the CDR.

1. Introduction

This Report provides external expert advice to the Data Standards Chair (**Chair**) in order for the Chair, in collaboration with the Secretary of the Department of the Treasury (**Secretary**) as Accountable Authority, to consider the best approach for Threat Modelling in the context of the Data Standards for the Consumer Data Right (**CDR**).

The CDR is an important national initiative and the Data Standards play an important role. In a complex fragmented system with multiple participants each creating their own software systems and operational processes, Data Standards ensure that everyone can interoperate. They instruct private sector actors, in designated sectors (such as banking), when and how to transfer personal and sensitive consumer data in particular circumstances. For example, the APIs in the current Data Standards ensure that the party sending data does so in the format that the party receiving the data expects and that steps in multiparty processes, such as authentication, are carried out consistently. Data Standards also play an important role in addition to that of ensuring interoperability. They ensure that an acceptable base line of security is followed by *all* parties in the ecosystem, whilst still allowing the individual parties freedom in how to implement the Data Standards on their own systems.

Security is crucial for the success of the CDR. Much of the data in the CDR ecosystem is sensitive, both inherently (as in the case of financial data) and because of what might be learnt from it (as where energy data is used to deduce household activities). A rich picture of individual lives, compromising privacy and facilitating identity theft, exclusion and manipulation or even enabling domestic violence, can increasingly be drawn from data circulating in an expanding CDR ecosystem. Once data is compromised, there is little that can be done to protect those affected. Even if data is only made public many years after a cyber incident, those to whom the data relates may still experience reputation and other harms. In addition, a data breach (whenever discovered) could substantially undermine the confidence users have in the CDR, and hence consumers' willingness to participate in the system. As a consent-based scheme, the success of the CDR hinges on the confidence of those participating in it – Data Holders, ADRs, Trusted Advisers, and consumers. The CDR thus depends on demonstrable reliability and security that generates justifiable confidence. For the digital economy to thrive, there is significant work to do in creating the conditions for such confidence.[5]

Security is also a government priority. Recognition of the cyber-Threat and overall disruption that may arise from a sophisticated cyberattack has been acknowledged in numerous contexts across government, with reforms enacted or being considered to better protect organisations, digital systems and individuals. Changes to the *Security of Critical Infrastructure Act 2018* (Cth)[6] require organisations responsible for critical infrastructure to have in place systems for identifying and managing risks. The Attorney-General's Department is conducting a review of *Privacy Act 1988* (Cth) with a view "to ensure privacy settings empower consumers, protect their data and best serve the Australian economy".[7] This builds on the Australian Competition and Consumer Commission's (**ACCC**'s) recommendations in relation to consumer privacy in the context of digital platforms.[8] Other policy initiatives include the release of Australia's '*Ransomware Action Plan*',[9] a draft national Data Security Action Plan,[10] and a report exploring ideas for cybersecurity regulations and incentives.[11] While these changes and proposals were announced prior to the election of the current Labor Government, the new Government continues to prioritise cybersecurity, including through a specific cybersecurity portfolio in the Ministry, and the announcement they are developing a new national cybersecurity strategy.[12]

Achieving effective and secure management of data in the CDR ecosystem requires understanding the Threats – who might seek to compromise the confidentiality, integrity or availability of data in the CDR ecosystem? Which Threat Actors might attack authentication or authorisation processes, compromise session integrity, or seek to lie or create false records about what has happened? What are their incentives to access consumers' information individually or in bulk, to alter data in transit or at rest, or to disrupt data flows? What is their capability to successfully carry out such attacks and what are the weak points in the system they may target to do so? Understanding Threat is essential for managing risk to the CDR ecosystem. Given the CDR is on the cusp of expansion to new sectors with potentially enhanced functionality,[13] the need to understand and assess existing and emerging Threats is critical.

In the context of this Report, a **Threat** is:

> Anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them.[14]

The use of "anything" and "objectives" here is notably broad because it is important in the context of enumerating relevant Threats to not overlook any factors which have the potential to cause serious issues, which in practice often arise from unanticipated directions.

Threats are generally entities (**Threat Actors**) or events. Threats target assets, they utilise attack vectors or **Vulnerabilities**, which are in turn mitigated by **Controls**. Threat Actors may have malicious motivations (in which case they can be described as **Attackers**) or may be operating accidentally or in error. Examples of Threat events include natural disasters, climate change and power failure. Assets affected by Threats can include tangible assets such as money or physical infrastructure, or intangible assets such as the achievement of objectives, reputation, or the availability and correct operation of processes.

The process of discovering and enumerating potential Threats is known as **Threat Modelling**. Several useful standardised ways of doing Threat Modelling have been developed over the past decades, and are known as Threat Modelling frameworks or Threat Modelling methodologies. Early methodologies focussed on enumerating specific attacks, other methodologies focus on the assets to be protected. In all cases it is helpful to understand the system, the assets to be protected and the types and capabilities of Threat Actors (see Section 3).

The term "Threat Modelling" does not have a universal definition, although there are common elements. Threat Modelling always includes identifying Threats and, to do this, there is a consideration of both the assets to be protected and the sources of Threats. However, the term is sometimes used to encompass additional activities, such as Threat mitigation through the use of controls. For the purposes of this Report, we have been asked to focus on the parts of Threat Modelling prior to the identification of controls, noting of course that the identification of controls, evaluation of the effectiveness of proposed controls, and decisions about measuring risk and prioritising of activities will then be required to follow this activity as part of a broader Risk Management Framework (**RMF**). To facilitate this overall security risk management process, the Threat Modelling methodology followed should incorporate a full range of activities to support Threat identification and assessment including asset identification (including evaluation of the sensitivity of the data) and Threat identification (including intent and capability of Threat Actors).

This Report outlines a range of accepted Threat Modelling frameworks and methodologies generally used in practice for Threat identification and recommends a structured approach for modelling the Threats to consumer data in the CDR ecosystem as the first stage in the security planning for the Data Standards.

Threat Modelling and the associated identification of Threats is one component of an RMF. An RMF goes beyond Threat Modelling as it quantifies risk likelihood and potential impact and enables informed risk management decisions including prioritisation, resourcing, and safety measures. The relationship between risk management and Threat Modelling in the context of security planning is explained in Section 4.2. This Report thus focuses on a single, but essential, component of the broader RMF.

While the primary responsibility for developing an RMF lies with the Accountable Authority of the Data Standards Body (**DSB**), currently the Secretary of the Treasury, the Chair has an important role. The Chair, as an official, has an obligation to weigh foreseeable risks before exercising their powers and functions – including in issuing Data Standards and making decisions about their content and binding nature. However, the Threats that impact on the CDR are not only of relevance to or preventable by the Chair. Some Threats might, for example, relate to risks best managed by the ACCC through processes used in accreditation of participants.[15] Indeed, the complexity of the regulatory framework for the CDR is part of the context in which Threats arise. Just as a Risk Report analyses how best to manage shared risk,[16] this Report makes recommendations as to how Threat Modelling can take account of Threats which present shared risks. Once the Chair understands what the Threats and associated risks are, the Chair will be in a good position to consider which risks they have a duty to mitigate through Data Standards and where there are opportunities to communicate and collaborate with other agencies to manage shared risks.

The remainder of the Report is organised as follows:

- Section 2 explains why Threat Modelling matters and why the Chair ought to engage in it. It also sets out the proposed scope for the Threat Modelling.
- Section 3 provides an introduction to the Threat landscape and Threat Actors for the CDR. It references Appendix A, which provides an analysis of attack types deployed by these Threat Actors.
- Section 4 describes Threat Modelling methodologies and explains our Recommendation 8 to use a synthesis of STRIDE and OWASP-TMP. These as well as alternative candidate Threat Modelling methodologies are analysed in Appendix B.
- Section 5 considers issues adjacent to Threat Modelling, including the need to establish and maintain an effective Threat Modelling capability, the need to rapidly respond to incidents based on proper security planning, and aspects of Threat related to the customer experience dimension of Data Standards.

FOR PUBLIC RELEASE

FOR PUBLIC RELEASE

2. Why Threat Matters
2.1 Threat in the Context of the CDR

The CDR was established in Part IVD of the *Competition and Consumer Act 2010* (Cth) (**CCA**) to enable consumers in progressively designated sectors,[17] commencing with banking, to authorise the sharing of information about them. As the CDR is rolled out in each sector, consumers can require information about themselves to be disclosed to themselves or to Accredited Data Recipients (**ADRs**). The scheme also provides for greater access to information in the relevant sectors that does *not* relate to any identifiable or reasonably identifiable consumers.[18] There are different sources of regulation for the CDR, specifically:

- Pt IVD of the CCA, which includes the Privacy Safeguards;[19]
- the CDR Rules made by the Treasurer;[20] and
- the Data Standards made by the Chair.[21]

The Chair has the power to make Data Standards about the following matters:[22]

a. the format and description of CDR data;

b. the disclosure of CDR data;

c. the collection, use, accuracy, storage, security and deletion of CDR data;

d. de-identifying CDR data, including so that it no longer relates to:

e. an identifiable person; or

f. a person who is reasonably identifiable;

g. other matters prescribed by the regulations.

'**CDR data**' is defined in section 56AI of the CCA. Classes of information are designated when a new sector is designated. Such information, as well as information wholly or partly derived from such information (including derivations of derivations), is 'CDR data'. For the banking sector, the classes of data designated include information about the consumer or their associate, information about the use of a product by a consumer or their associate, and information about a product.[23] Each element of CDR consumer data is linked to a CDR consumer being the identifiable (or reasonably identifiable) person to whom it relates because of the supply of a good or service to that person or an associate. CDR data is not always personal or sensitive because it does not always relate to a CDR consumer. For example, in banking, it can include product reference data. However, CDR data that relates to CDR consumers can be sensitive.

In essence, the CDR scheme requires incumbent suppliers that hold CDR data in respect of a consumer (**Data Holders**) to transfer CDR data to certain third parties upon the consumer's request, with the goal of permitting those third parties to use that data for the consumer's benefit in providing some service or offer expressly requested by the consumer. These might include, for example, comparison services, budgeting products, alternative offers on personal loans, or energy plans. To receive CDR data in this way, the third party must generally meet legislated requirements in order to be accredited by the ACCC as an ADR.[24] 'Trusted Advisers' (satisfying the conditions in CDR Rule 1.10C) nominated by a consumer can also receive CDR data from an ADR with the consumer's consent.[25]

The data security elements of the Data Standards currently focus on API design and when and how data is transferred between Data Holders and ADRs. There are no specific requirements around physical infrastructure other than the need to meet the articulated requirements. There are no specific requirements currently around endpoint security; the focus is on data in transit from Data Holders to ADRs, not on data in transit to Trusted Advisers nor data at rest (data electronically stored by or on behalf of Data Holders and ADRs).

Different industry sectors have different underlying cybersecurity maturity. For example, banks are heavily regulated and have a long involvement with and strong existing capability in security that may not apply to all CDR participants. The security of data at rest is thus likely to vary widely across the CDR ecosystem.

While the CDR involves many intersecting parts (including legislation, rules and accreditation processes), Data Standards are at the centre of when and how data is managed and protected across the CDR ecosystem. They are thus central in creating the conditions for the privacy of consumers and the security of CDR consumer data. Data Standards should be trustworthy and reflect best practice, and, in particular, should protect consumers from a growing range of cyber Threats that might target them and their data. Those responsible for the Data Standards can only do this effectively if they are aware of and understand those Threats. In other words, understanding what threatens the security of data in the CDR ecosystem is an essential first step towards identifying, analysing and mitigating risks associated with responsibility for Data Standards.

Data Standards have the potential to impact on the security of CDR data, in particular in relation to confidentiality, integrity, availability, and authentication. Confidentiality protects a consumer's privacy in the information also reducing their susceptibility to identity fraud and social engineering. Integrity helps ensure that decisions and actions affecting consumers are based on accurate information. Availability is essential for the functioning of the CDR, ensuring that data flows through the CDR ecosystem in a timely manner and in accordance with the CDR Rules and Data Standards. Authentication ensures that parties sending and receiving data, and consumers providing consent and making requests, are who they claim to be. All

these elements are necessary to enable participants in the CDR to carry out their intended activities and to provide the services to consumers the enabling of which is the purpose of the CDR. The security of consumer data in the CDR ecosystem is a thus critical element of the Data Standards.

Because it is consent-based, consumer confidence in the security of the CDR ecosystem is essential for the success of the CDR in achieving its goals (such as improving competition in particular market sectors). Perceptions around security risks of participation can therefore be as important for the success of the CDR as avoiding actual data breaches. The willingness of consumers to participate in the wider digital economy, including the CDR, depends upon those consumers having confidence in the safety and privacy of their data. If there are publicised data security breaches or public criticism by experts suggesting that the levels of data safety and privacy are less than expected by consumers, then it is difficult for digital data ecosystems such as the CDR that rely upon public opt-in to succeed. It is worth pointing out here that relying upon attempts to keep data breaches or security flaws secret is not a solution because keeping such information secret would itself undermine consumer confidence (as consumers would not necessarily assume an absence of data breaches in the absence of transparency). The adoption of data breach notification in Australia reflects the reality that secrecy about security issues does not assist security or increase confidence in security.[26]

Changes in the CDR regime, coming with extension of Data Standards into new industries and new functionality, also changes the Threat surface. Further Threat Modelling will need to be undertaken as part of the process for conceiving, developing and implementing changes in the CDR regime. First, there are plans to extend the CDR into new sectors. The CDR began as "open banking" with the first extension being into energy. It seems likely that it will soon include telecommunications and non-bank lending. In October 2020, the Australian Government published *Future Directions for the Consumer Data Right* which recommended that the functionality of the CDR expand in various ways. While the recommendations are extensive, some elements most relevant for highlighting potential impact on Threats include:

- Rather than simply requiring organisations to share data (read access), consumers will be able to authorise others to initiate actions (write access), including switching providers and initiating payments (**Action Initiation**). This expansion would apply sector-by-sector, again starting with banking, with each expansion subject to a sector assessment (that, in our view, should include impact on Threat). This would be bolstered through additional authorisation processes and accreditation tiering. While this would be implemented in legislation, there would be delegations including to the Chair.
- The CDR is to operate more flexibly (including in selection of datasets, flexibility in sector assessments and reciprocity in sharing).
- Unaccredited and lower accredited third parties will be allowed to collect and disclose data on behalf of an ADR.
- Coordination with similar frameworks internationally will be enhanced, including cross-border data flows.
- More information will be available for consumers, including a dashboard displaying who they are sharing data with, how it is being used and an ability to make changes or withdraw consent.

These changes, if implemented, would have a significant impact on both the scope of the Data Standards and the nature and impact of Threats. In our view, changes in either the scope of the CDR (to new sectors) or the functionality of the CDR should prompt new or revised Threat Modelling.

Due to the nature of the current cyber security Threat landscape, it is a question of when, not if, there will be a CDR data breach. A widely publicised data breach has the potential to damage public confidence in the CDR ecosystem, and perhaps government more broadly, and in addition harm consumer privacy. This would impact future take-up and use.

To better assure security of CDR data and hence the viability of the CDR, it is necessary to understand what could go wrong. Effective security planning thus involves following ongoing processes to understand:[27]

1. what needs protecting;
2. what the Threats are; and
3. how people, information and assets will be protected.

This Report is concerned with the second of these, which depends upon consideration of the first.

2.2 Threat Scope from the Perspective of Chair

From the perspective of the Chair with power to make Data Standards on the matters set out in CCA s 56FA(1), copied in Section 2.1, the relevant Threats are those which have impact on the security of CDR data, the broader CDR ecosystem and the viability of the CDR itself. This section analyses the scope of such Threats which ought to be in the Chair's view.

There are three dimensions of scope that need to be analysed. The first (Section 2.2.1) relates to the CDR data lifecycle. For example, ought the Chair only be concerned with CDR data *in transit* between a subset of the participants in the CDR scheme or more broadly with Threats to CDR data in the hands of all participants (*data at rest*)? The second (Section 2.2.2) relates to the context for Threat Modelling, in particular whether that context includes the complexity of the regulatory and governance framework for the CDR and the CDR ecosystem as a whole. The third (Section 2.2.3) relates to the kinds of Threat that should be considered and, in particular, whether the Chair consider *all* Threats with potential to harm the CDR. This contrasts with a position whereby the focus would be exclusively on the Data Standards – in terms of data lifecycle (limited to data in transit), context (limited to the role of Data Standards) and Threats (limited to Threats arising directly from current Data Standards and decisions to issue new Data Standards).

In each case, in considering the security of CDR data and how to assure it, we recommend that the Chair consider the full range of Threats. It is important that the range of Threats be as comprehensive as possible because security is a *weakest link* phenomenon. For example, there is limited use in securing the doors of a house with security controls such as locks if the Threat of window entry is overlooked, and the house has large, unlocked ground level windows.

Regardless of whether a narrower or wider lens is chosen, enumerating the full set of Threats to the data should not be regarded as being a trivial or routine exercise. A truism in security is that successful attacks do not involve those Threats which have been well understood and well defended. The challenge in Threat discovery and enumeration is to notice as many of the unknown unknowns as possible whilst not accidentally overlooking any of the known knowns.

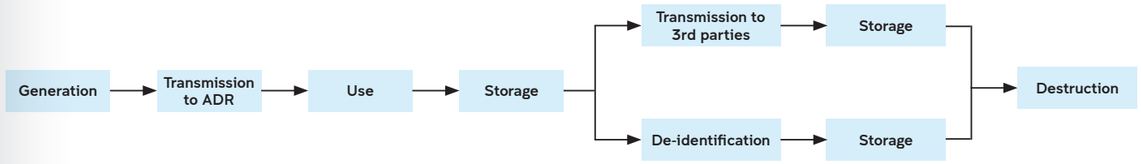
To help defenders come up with as comprehensive a Threat list as possible, a range of Threat Modelling frameworks and methodologies have been developed over time. These frameworks and methodologies serve as an aid to help prompt consideration of common Threat categories so as not to overlook these sorts of relatively well-known Threats. They should be coupled with an approach to wide and effective consultation with experts, users, and those involved with building, operating, and leading all the various aspects of the system, so as to gather specialist insights into (1) what are the assets to be protected, and (2) the detailed nature of the potentially vulnerable elements of the system. Diverse and effective consultation is essential to help discover unknown and unfamiliar Threats specific to the particular nature and context of the system and its diverse elements.

The CDR has network value; the benefits it provides increase with the amount of data it can provide. A loss of public confidence and reduced uptake of the system by consumers would diminish the benefits of the system and seriously threaten its overall viability. Threat Modelling should thus be done with a wide lens and shared among all stakeholders so that, collectively, risks associated with Threats can be identified, analysed and managed.

2.2.1 The CDR Data Lifecycle

The lifetime of data in any system can be broken down into distinct phases, sometimes collectively known as the data lifecycle. These include the collection, use, storage, and eventual deletion of the data.[28]

Figure 1: The CDR Data Lifecycle



In the context of the CDR, the data lifecycle commences once a consumer is authenticated and authorises the transmission of their data from a Data Holder to an ADR. Once that transmission occurs, the consumer's data is then used and likely stored by the ADR in order to provide the consumer with the services or information which they have requested. While being used or stored, the data may be sent to or accessible by third parties such as cloud providers or backup services used by the ADR. Consumer CDR data might also be transmitted, with consumer consent, to a third party Trusted Adviser. Once the data is no longer needed for the purpose for which its use was authorised or the period for which its use was authorised has expired, the ADR must safely destroy or de-identify the data. This must also be done upon request by the consumer.

Securing Data over the Data Lifecycle

To ensure the security of data in a system, is necessary to secure it throughout every phase of the data lifecycle. Therefore, to secure CDR consumer data, it is important to adopt a holistic approach spanning the entire lifecycle and not simply focus on security of the data in some phases in the life cycle. For example, it would not make sense to encrypt consumer data while it is in motion from a Data Holder to an ADR if the ADR were to process such data in plaintext using hard disks which are then sent to insecure recycling at the end of their lifetime.[29]

The CDR data life cycle is more complex than the data life cycle of many single party systems where data, once received, often stays in-house. In the CDR, there are two additional complexities: third party data transfers and de-identification. Data received by an ADR and stored in their safe custody may subsequently be copied and transmitted to third parties, such as Trusted Advisers. Data held by a CDR participant may be de-identified and then treated under different security arrangements than non-de-identified data. For example, after being de-identified, consumer data is not subject to the same requirements for eventual deletion, and the use of that data is not restricted to the uses which the consumer initially authorised.

It is important that these and any other variations from a simple traditional data lifecycle are governed by processes with the same level of security that applies over the other phases of the lifecycle. If these parts of the lifecycle are ignored from a security perspective, Attackers will simply target the data in the phase when it is least well secured. As noted above, this is one aspect of the *weakest link* phenomenon.

Currently, the Data Standards target the security of the transmission phase in the data lifecycle, setting the security standards for authentication and data exchange between a Data Holder and an ADR. We suggest the Chair consider the potential to write further Data Standards to govern the minimum security standards for the consumer data throughout the entire data lifecycle. This is within power, and for example Data Standards may relate to the "security and deletion" of CDR data.[30] Unless Data Standards consider the full lifecycle of CDR data, that data may be briefly secure whilst being transferred between a Data Holder and an ADR but then be compromised at a later stage.

It is worth the Chair considering, in particular, whether there should be a minimum security standard for secure data transfer between an ADR and a Trusted Adviser. It might be seen by the public as unexpected that their data is secured on the first leg of its journey but then is insecure when transmitted to their Trusted Adviser. Given that Trusted Advisers may well be organisations of considerable size with access to a considerable volume of data, it seems inconsistent for the Data Standards to be silent on the security of the consumer data when provided to a Trusted Adviser. In our view, this should go beyond customer experience standards for disclosure of CDR data to Trusted Advisers.[31]

The security of data after de-identification is currently assumed. However, data de-identification is a new and emerging field with potential capabilities still not well understood or generally accepted. It is often straightforward to demonstrate a method which can re-identify data which has been classified as "de-identified". One well known example is the Medicare health

2.2 Threat Scope from the Perspective of Chair (continued)

data which had been claimed to be de-identified before being released but was easily re-identified by researchers using dates of birth and dates of admission of mothers to maternity wards in hospitals as a point of reference.[32] On the other hand, it is considerably harder to be confident that *no* re-identification method exists for data sets when one has not yet been found. Re-identification methods are likely to continue to develop and become more powerful over time. The current de-identification framework[33] does not deal sufficiently with these challenges.

From a security perspective, the security and privacy preserving nature of de-identification methods can only ever be regarded as provisional. There remains an ongoing risk that a sufficiently determined and well-resourced Attacker will re-identify "de-identified data" in the future, particularly in conjunction with other data sets which might become available in the meantime. This consumer data privacy risk will remain even where consumer data was originally de-identified using the best practices available at that time.

There is a tension between the role that de-identification plays in the CDR and the security reality. The Chair has power to issue standards with respect to de-identification, but de-identified data is seen as an exit path. For example, in Privacy Safeguard 12, entities are given the option of destroying or de-identifying data, despite the fact that, in reality, one of these pathways has significant ongoing security risks. The primary lever for the Chair relates to the process of de-identification itself rather than an ability to make Data Standards for the ongoing storage and eventual deletion of de-identified CDR data.

Nevertheless, it remains important for the Chair to understand the security risks associated with attacks on de-identified CDR data. There remains a potential for the Chair to respond to such risks by tightening Data Standards relating to de-identification, albeit within the constraints of the CCA and the CDR Rules. Further, the Chair may wish to collaborate with other stakeholders within government and included industries about how de-identified CDR ought to continue to be protected in an ongoing manner after a de-identification process has occurred.

2.2.2 Threat Context: Complexity

The context of a system has a critical bearing on the nature of the Threats to which they will subjected. It determines the environment in which Threat Actors will operate and hence the Threats that they generate. Further, context influences the way that the systems are built and operated and hence the vulnerabilities which will be exposed to attack.

The most salient aspect of the security context in which the CDR operates is its complexity.

The CDR is extremely complicated. Its operation involves multiple parties including Data Holders such as banks, ADRs, Trusted Advisers, consumers, and regulators. The governance and security responsibilities for the system are fragmented with different and quite separate bodies responsible for parts of the system including the ACCC, the DSB, and the OAIC. In addition to the CCA, there are CDR Rules and Data Standards, all created and administered by different bodies. The number of parties involved coupled with the fragmented nature of the oversight poses a considerable challenge to being able to achieve a coherent and well-integrated security posture for the CDR. The current complexity of CDR is likely to be one of the main enablers of Threats to ongoing security of CDR data.

A lack of transparency and common understanding is a further significant environmental root cause of vulnerabilities and consequent Threats in cybersecurity. The decentralised and complex system of participants in the CDR is confusing for ordinary consumers to understand, yet the consumers do need to understand the system in order to meaningfully consent to and securely authenticate the safe sharing of their data. This potential for misunderstandings has important consequences for consumers as social engineering attacks and scams (discussed in Section 3) work by exploiting gaps in the understanding of individuals.[34]

Furthermore, consumers will likely expect that the system is a government system, and some will therefore place a high degree of confidence in it. Consumers might get this impression from CDR web pages that, for example, "[t]he data transfer is done between the providers, but the Australian Government oversees the overarching framework."[35] Yet, in practice, the system is a series of proprietary software systems written by individual participants, with the government input being rules (including Data Standards) that are implemented by other participants.

There is insufficient openly available information available to allow us, as external experts, to assess with confidence the degree to which the numerous software implementations in the system currently comply in practice with the CCA, CDR Rules and Data Standards. We thus cannot assess the degree of confidence that can be placed in the ongoing quality assurance and audit processes to ensure that software and systems and internal participant procedures and data handling practices remain safe and compliant. If we are unable to satisfy ourselves, it follows that the challenge would be much greater for general consumers.

That said, the open and transparent manner in which the standards have been developed and managed is an excellent example of best practice in transparent open collaborative development. All versions of the Data Standards submissions, and conversations with logs and timestamped versions are

shared on GitHub, and are made available to the public.

The highly fragmented nature of the CDR environment and its resultant complexity and potential gaps in consumer understanding are not within the remit of the Chair to address. However, given the significant extent that these factors lead to an environment which fosters Threats to the system, we believe that the Chair ought to be aware of the security implications they pose. This is because the complexity of the CDR (both the legal and regulatory framework and the CDR ecosystem) is likely to be one of the most serious factors imperilling the ongoing security of CDR data.

2.2.3 Sources of Threat

As an aid to not inadvertently overlooking Threats, Threat Modelling should consider as many as possible of the *sources* of Threats that have the potential to compromise CDR data or cause harm to the CDR. These sources of attack are collectively known as the Threat landscape.

The major elements of the Threat landscape arise from human adversaries, or Attackers, who might be the source of attacks. Other, non-adversarial, sources of Threat also need to be investigated during modelling.

Attackers

Attackers working alone or in groups will be the principal source of Threats to the security of CDR data. Because of their centrality to the Threat landscape, they are the focus of Section 3, which considers the different categories of Attackers in more detail. Here we consider their potential motivations to attack the CDR.

The volume of data about consumers circulating in the CDR ecosystem is hitherto unprecedented in Australia. Available CDR data initially includes high quality authenticated financial data on all Australian customers for all banks, on an ongoing basis. The CDR is already expanding to include energy data and will likely extend further. The increasing volume of data available through the CDR ecosystem will be extremely attractive to Attackers such as Cybercrime Groups, Nation State Actors, and Trusted Insiders. Each of these may find value in the data. For example, they may use the data for ransomware or blackmail purposes, for background reconnaissance for targeted cyber attacks or bulk phishing campaigns, for targeted advertising and consumer manipulation, for influence campaigns, as well as for helping facilitate identity theft, scams, and associated cybercrimes. Because the data is valuable for such purposes, it might also be stolen for the purposes of on-selling.

The CDR is also an attractive target to attack to cause disruption. Over time the more central the CDR becomes to the digital economy and the more data flowing through the system, the greater the potential for an Attacker, such as an activist, terrorist, or extortionist, to cause disruption.

Finally, the infrastructure of the CDR itself provides a gateway to multiple organisations and institutions. It may be that Threat Actors seek value by obtaining credentials and using CDR mechanisms to carry out crimes. For example, if Action Initiation is added to the CDR functionality (as has been foreshadowed) then Attackers could use the CDR to carry out money transfers and so directly steal from consumers. Attackers might also use Watering Hole Attacks which are where well-resourced Attackers compromise web sites to deliver malware or misinformation to high value visitors. Such attacks could compromise pages within the CDR ecosystem to attack privileged, or administrator-level staff of participant organisations who view the pages, potentially leading to the compromise of internal systems of CDR participant organisations.

Threats from other sources

Although Attackers will be involved in most potential Threats to the CDR, it is important to also consider Threats from sources other than human adversaries. These might relate to accidents, disasters or the environment.

In any complex system, the chance for accidents including those arising from human error is significant.[36] It is important that the enumeration of Threats include consideration of the possibility of errors being made by any of the participants in the system, including for example by consumers, software developers, and accreditors. The possibility of accidents and disasters arising from other causes should also be considered – for example power outages, extreme weather events, or equipment failures.

In general, where an accident can happen by chance, a sufficiently resourced Attacker could also cause the same thing to happen by deliberate malicious action. So, in practice, Threats identified by the consideration of accidents should also be included in the consideration of adversarial Threats.

The contextual factors discussed in Section 2.2.2 can also be viewed as sources of Threats. Individual Threats can be enabled by, or amplified by, system complexity, and by insufficient capability to support internal security functions including over-dependence on key employees (discussed further in Section 5.1).

2.3 Incident Scenario

This section sets out a hypothetical scenario in order to demonstrate why Threat Modelling is important. Scenarios such as this should be used as part of the formal Threat Modelling activity. By considering the scenario, it is possible to identify actions that might be taken now, as part of an RMF, to reduce the likelihood or impact of the hypothesized Threat. Although the scenario itself is hypothetical, it involves a real cybercriminal group and their actual capabilities and behaviours..

2.3.1 Attacker Capability and Intent

The advanced Eastern European Cybercrime Group known as Wizard Spider[37] is primarily based out of Saint Petersburg in Russia. Russia is suspected of tolerating, or even assisting them.[38] They are known to target CDR industries, including: energy, finance, telecommunications, and government. They are also known to target Australia and New Zealand. Wizard Spider have demonstrated the capability and proven their intent to sell access to sensitive data to criminals. They are a criminal group responsible for the development and distribution of complex and varied software tools specifically designed for the compromise of systems and exfiltration of data from them. These tools have been used in several sophisticated cyber operations. Financially motivated cybercrime remains the largest component of the cyber-Threat landscape, and Wizard Spider's business model is to service this market. Wizard Spider are suspected to be behind the largest known attack against a health service computer system, in the Republic of Ireland. They pose a clear Threat to the security of the CDR consumer data.

Consumer data can be used to extort and compromise individuals. Just as 22.1 million records held by the US Office of Personnel Management were subject to a data breach by a Foreign Intelligence Service in 2015,[39] it is possible that a Foreign Intelligence Service could commission Wizard Spider to obtain CDR data for political purposes.

Wizard Spider has been targeted by Europol, Interpol, FBI, and the UK's NCA, but Wizard Spider is very security conscious, only deals with trusted criminal organisations, and does not openly advertise its criminal services on the Dark Web.[40]

The CDR is enabled by default for any consumer with an account with a Data Holder, including the major and second-tiers banks. Therefore, if Wizard Spider were to attempt an attack on Australian banking data, they would likely investigate the CDR as a potential access point. This is because banking CDR data would otherwise be protected by bank-grade cybersecurity infrastructure, operations, and Threat intelligence.

Below is a hypothetical incident scenario highlighting a potential attack by Wizard Spider on CDR data. The potential attack outlined in the scenario would not be particular to Wizard Spider alone. There are over 100 advanced-capability cyber adversarial groups being tracked by Threat intelligence researchers and analysts, of which Wizard Spider is just one example.

2.3.2 Incident Scenario

Wizard Spider could compromise the CDR via an ADR using an unknown Zero-Day exploit (attack tool) they have purchased, or by exploiting a known vulnerability that has not yet been remediated.

For the purposes of this simulation, suppose Wizard Spider have successfully targeted an ADR, in this case a large and rapidly growing Australian Fintech company. They have gained access to the company's IT systems by taking advantage of the infamous Log4Shell vulnerability, a known vulnerability in one of the company's systems which was not patched quickly enough.

Log4Shell existed as a vulnerability permitting criminals to log into affected systems from 2013 until being made public in 2021, affecting approximately 93% of all enterprise cloud environments. Given the prevalence of the vulnerability, Log4Shell continues to be exploited by cybercriminals against organisations which have not patched it. Wizard Spider would likely first attempt all publicly known vulnerabilities against targets, and then sparingly deploy their secretly known Zero-Days to compromise the CDR via an ADR.

The Fintech company is an ADR with a large daily volume of CDR data. After obtaining access to the company's systems and then exploring them for the past two months without being detected, Wizard Spider extracted copies of the sensitive data they have discovered and then encrypted all the data and all the software on the systems. This has had the effect of taking the Fintech company offline and rendering all their IT systems completely unusable. It is also possible that Wizard Spider have been able to obtain the company's CDR authentication credentials.

Wizard Spider demands the Fintech company pay a ransom of $1 million in Bitcoin to obtain the decryption key need to restore their systems. If the company does not pay within 7 days, Wizard Spider will publish all the sensitive data they have stolen, including CDR data. To show that they have obtained sensitive data Wizard Spider immediately publishes some financial details of several high-net-worth Australian businesspeople and politicians.

From the perspective of the CDR, this attack involves:

- a confidentiality compromise of CDR data,
- the risk of Wizard Spider impersonating the Fintech company in interactions with other CDR participants, and
- a disruption in the ability of consumers to access the CDR data related services of the Fintech company.

In the STRIDE Threat framework, which is discussed in Section 4.5, these would be classified as *Information Disclosure*, *Spoofing*, and *Denial of Service* respectively.

2.3.3 Commentary on the Incident Scenario and how it informs the Threat Modelling process

Considering Threat scenarios such as this one during Threat Modelling is an essential step in enhancing security. Open ended but realistic scenarios can be a powerful and motivating prompt to security planners when working to identify and assess Threats. In particular, it is important that any weaknesses identified in the scenario are understood so they can be generalised and remedied, including where relevant through amendments to the Data Standards (and/or CDR rules).

Depending on the nature and scale of the CDR Data that Wizard Spider stole and/or discloses publicly, there could be an **extreme impact** to individuals, and/or those associated with them, of serious damage from discrimination, mistreatment, humiliation or loss of dignity or safety.[41] For example, there may be loss of life of an individual or small group, perhaps as a result of suicide, domestic violence or criminal reprisals, a risk that ought to be assessed as 'high' likelihood.[42] When user data including credit card numbers and transactions from the Ashley Madison adultery website was breached and made public the impact on some affected individuals included resignations, divorces, and a small number of confirmed suicides.[43]

In the scenario, as in a real-life incident, it may not be clear how the Attackers obtained the CDR data. Wizard Spider may have exploited a protocol or implementation weakness in the way the data was transmitted between Data Holders and the Fintech company; or it may have been a weakness in how the company encrypts and stores the data; or Wizard Spider may have observed the data in the company's systems while it was not encrypted; or some other method. In a real incident, this uncertainty would need to be resolved rapidly to know what remedies are required. For example, there many need to be an urgent change to the cryptographic processes set out in the Data Standards.

Because of the impersonation risk, it would be important that there is an established process to ensure that all participants in the ecosystem immediately stop trusting the Fintech company's credentials. The Chair could ask now – are there processes for rapid responses to incidents, including urgent changes to Data Standards and prompt exclusion of compromised CDRs from the CDR ecosystem?

This incident would be likely to generate media attention and publicity and has the potential to seriously undermine public acceptance of the CDR and the public's willingness to use it. The Chair could ask now – how would this be handled?

In a scenario such as this, it is worth considering the different objectives of the Chair and the compromised entity or entities. The Fintech company's top priorities would probably be getting the intruders out of their system and getting their systems back online. They would be concerned about reputational damage from the incident but informing the Chair or preserving the secrecy of the leaked CDR data may well be of secondary importance to them. One could ask now – what mechanisms exist to ensure the most relevant government Actors (the Chair, ACCC and OAIC) are informed and able to respond to incidents affecting the security of CDR data during an incident? This raises analogous questions to the recent critical infrastructure reforms; in both cases, government has an interest in exercising control over private organisations in particular circumstances.

2.3 Incident Scenario (continued)

The Australian Government's general approach to cyber extortion is to not pay ransom demands.[44] However, this may well be softened if there are security or safety considerations were the data to be published. It may be that an argument could be mounted that the ransom should be paid. Individual companies are free to pay ransoms if they choose except where prohibited by law (in this hypothetical case it would be important to determine whether Wizard Spider is impacted by current Russian sanctions for example), but are required to disclose certain data breaches to the Privacy Commissioner and/or data subjects. One could ask now – would a ransom be paid if the functionality of the CDR or privacy of consumer data were at stake? Note that paying the ransom would not eliminate risk to CDR data; security researchers have found cases where Wizard Spider has retained copies of extracted data even after a ransom has been paid.[45]

It may not be possible to determine which CDR data or consumers are affected by the attack. So it may be unclear who the Fintech company needs to notify. They would probably err on the side of caution. The Chair could ask now – how *should* this be managed collaboratively among the Fintech company and relevant government agencies? Is there a useful role for Data Standards?

In the aftermath of a successful attack, it will not be immediately obvious if the Data Standards were at fault. Regardless of which vulnerability is determined to have been exploited, the Data Standards may need to be modified, or a statement may be required from the Chair, to repair and restore confidence in the CDR. This would need to be done quickly. The Chair could ask now – Is it necessary to have a Data Standards Safety System to manage rapid responses and changes to the Data Standards in the event of an attack?

To reduce reputational damage, the Fintech company may announce that they followed all CDR Rules and Data Standards. They may even be able to produce expert reports confirming this. If so, the reputational damage may fall on those responsible for these, including the Chair, as they may not have provided the expected protection. This potential for an event to undermine confidence in the CDR, the digital economy, or even government more broadly, is a critical risk that should be identified and managed as part of an RMF.

Consumers subsequently affected by identity theft and other losses which occur after the time Wizard Spider gained access to the Fintech company's systems may believe that the CDR breach was responsible for, or contributed to, identity theft causing them financial harm. They may well be correct, however in many cases it will be impossible to confirm. This may attract wide media attention. The potential for direct consumer harm as well as the secondary reputational consequences for the CDR should be identified and managed as a shared risk in the RMF.

A number of weeks (21-day average in Asia Pacific region in 2021) usually go by before successful cyber attacks are identified.[46] Often this discovery is too late, with criminals announcing themselves only after they have successfully exfiltrated data, deployed ransomware, or performed some other visible offence.

Note that in reality, just as in this scenario, the question is not whether an Attacker, such as Wizard Spider, would attack the CDR. They would. The more useful question is what should be done *before* they do. Considering scenarios such as this as a component of an overall Threat Modelling activity can point the way forward in identifying what should be done now, both in the context of the RMF and in context of other measures, such as a Data Standards Safety System.

3. The Current Landscape of CDR Threat Actors

As discussed in Section 2.2.3, while there are a variety of different Threat *sources*, Attackers, being human adversaries, are involved in most Threats. This section describes the current Threat landscape through a consideration of different types of Threat Actors, focussing on Attackers.

The CDR will be attractive to a range of human Attackers with a range of motivations. The CDR provides potentially porous digital communication connections between a diverse range of organisations and individuals and, by design, accumulates and transfers significant volumes of sensitive consumer and product related CDR data. Against this background, Attackers who compromise the CDR or who are able to exploit CDR participants can achieve malicious objectives ranging from monetising a successful intrusion (including through an extortion demand following ransomware deployment as seen in the Incident Scenario in Section 2.3.2), obtaining unauthorised access to CDR data, pursuing political objectives, obtaining leverage for coercion, gaining notoriety, supporting foreign initiatives (including disrupting the digital economy or trust the government), or causing deliberate harm to targeted CDR participants.[47]

It is critical to identify and predict the likely actions and techniques used by Threat Actors to ensure the overall success of the CDR and protect individual consumers and other parties involved in the CDR ecosystem. Accurately understanding Threat Actors also provides critical insights into the effective design of defensive CDR Data Standards and controls that best limit attacks and mitigate Threat Actor impact.

There is no universally agreed way to categorise Threat Actor groups within the cybersecurity community. For the purpose of this Report, we have focused broadly on malicious actors with proven track records of compromising systems of significant national interest. There is discussion of both Threat Actors who have clearly identifiable motivations to compromise Data Holders, ADRs, Trusted Advisers, and consumers, but also more broader considerations of Threat Actors in the current landscape. Consideration has also been given to non-malicious behaviours of CDR participants which may create cybersecurity Threats or may enable exploitation by malicious Threat Actors. Under this framework, five key Threat Actor types emerge as most relevant to the CDR, being:

- Nation State Actors;
- Cybercrime Groups;
- Competitive Intelligence Threat Actors;
- Trusted Insiders;
- Hacktivists.

Each Threat Actor type is described and analysed in the next page.

3.1 Nation State Actors

Given the amount of sensitive, verified, and aggregated data held by Data Holders and ADRs, and the critical nature of the industries included, the CDR will be a key target for hostile nation states and the Actors that conduct activities on their behalf, including foreign intelligence services and state-sponsored hacking groups.

While hostile cyber activity and espionage between nation states is not new, the era of big data and digital disruption has created an environment in which individuals and private sector entities are now common targets of nation state cyber activity.[48] A recent CSO report identified that 35% of Nation State Actor cyberattacks are now carried out against enterprises,[49] and are increasingly responsible for supply chain cyberattacks.[50]

Nation State Actors have been designated by the ACSC as the most significant Threat to Australia's national security and economic prosperity.[51] These Threat Actors differ from Organised Cybercrime groups in a number of ways including:

- possessing higher levels of training, motivation, and resources;[52]
- adopting an approach that is more mission-focused and persistent – for example undertaking long-term research, scans and probes of potential targets. In some cases, they may focus on a single task for many weeks, months or years;[53]
- having a 'licence to hack', meaning they are working within legal guidelines of their own state and are less likely to be concerned with consequences of their actions;[54] and
- stealth and covert capabilities allowing them to avoid detection and identification.[55]

Nation State Actors typically undertake a broad range of malicious activities designed to further the state's political aims and interests.[56] These activities often include cyber espionage, stealing sensitive data, intellectual property and/or classified information, infiltrating and gathering intelligence about a sovereign nation's cybersecurity and resilience capabilities, compromising key IT and physical infrastructure, and undertaking long-term surveillance activities.

Nation State Actors will target the CDR for cyber espionage, destructive purposes or for financial gain, including:

- **Exfiltration and exploitation of CDR data for intelligence purposes:** Nation State Actors would be aware that CDR data is high-quality and verified, thereby increasing its utility and value. Gaining access to and exfiltrating CDR data, including the personal information of individuals, would mean access to the personal information of government officials, high-profile and/or politically exposed persons as well vulnerable, and high-risk individuals such as those fleeing oppressive regimes or political, racial, religious, or social persecution. While CDR data itself may not be enough to enable Nation State Actors to leverage, coerce, groom, blackmail, or manipulate these individuals for espionage purposes, when combined with other sources of data or information, its intelligence value increases significantly. In 2019, the Australian National University was attacked by a suspected Nation State Actor which gained unauthorised access to and exfiltrated large volumes of students' personal information which could be used for a wide range of intelligence purposes; [57]
- **Reconnaissance and intelligence gathering** of data relating to the network security architecture of the organisation for future attacks;[58]
- **Theft of intellectual property or business intelligence:** While it is unlikely CDR participants would store or have access to state secrets or classified information, it is highly likely Nation State Actors would seek access to confidential business information including intellectual property or business intelligence for economic gain, competitive advantage, or political reasons.[59] Nation State Actors targeted Australian Government departments during the COVID-19 pandemic, searching for information related to Australia's response to the pandemic.[60] The United Kingdom's National Cyber Security Centre also identified attempted entries to access data relating to COVID-19 vaccine formulation.[61]
- **To disrupt, compromise or destroy victim IT environments or signal intent** and to target sectors of critical importance.[62] In mid-2019 to early 2021, Russian General Staff Main Intelligence Directorate (**GRU**) military unit 26165, conducted widespread, distributed, and anonymised brute force access attempts against hundreds of US government and private sector targets worldwide to compromise enterprise and cloud environments.[63] In July 2021, the US Government attributed a synchronised and coordinated 2015 cyber campaign against Ukrainian critical infrastructure, including Ukrainian power companies, to Russian Nation State Actors;[64]
- **To erode public confidence** in the CDR regime, or the digital economy more broadly, and by extension the Australian government;
- **For financial gain:** Sanctioned nation states such as North Korea increasingly rely on illicit activities like cybercrime to generate money and evade United States and United Nations sanctions.[65] That could include selling hacked

3.1 Nation State Actors (continued)

CDR data on the Dark Web or stealing virtual currency from software wallets and cryptocurrency exchanges. In March 2022, the US Treasury attributed the hack of a blockchain project linked to the online game Axie Infinity to North Korean state-sponsored hacking group, Lazarus Group.[66] Virtual currency worth USD$620 million was stolen by Lazarus Group;

- **Retaliatory cyberattacks** in response to external events such as cyber or kinetic war or other geopolitical events. Recently, Lithuania was the target of several Russian nation state cyberattacks in retaliation to restrictions imposed on cargo traffic to Russia (imposed following Russia's invasion of Ukraine).[67] These attacks were launched on various public Government and private organisations, causing disruption to numerous websites through a distributed denial of service attack on a national data network.[68] The ACSC warned of similar Threats to critical infrastructure.[69] Another example of the potential for retaliatory cyberattacks would be the ongoing US intelligence agency warnings of potential Iranian cyberattacks against private sector and government entities following a US drone strike that resulted in the death of Iranian General and commander of the Quds Force, Qassem Soleimani.[70]

Nation State Actors will make use of a variety of tactics, techniques, and procedures to gain unauthorised access to IT environments to achieve their objectives. Nation State Actors are capable of adopting all of the common attack methods described in Appendix A. The most likely nation state attacks against CDR participants will include:

- **Watering holes:** Where Attackers infect legitimate websites that a victim is known to visit, for the purpose of delivering malware or misinformation to them;[71]
- **Spear-phishing:** The targeting of specific (as opposed to all) individuals with fraudulent emails, messages, texts and/or phone calls to steal login credentials or other sensitive information;
- **Zero-day exploits:** The use of unknown security vulnerabilities or flaws in software prior to the discovery and patching by the developer or IT team;[72]
- **Inside actors or insider Threats:** For example, where a Nation State Actor convinces a CDR participant's employee or contractor to share or sell information or access to IT systems.[73]

Nation State Actors are likely to attempt API data scraping against CDR participants. API compromises are a key emerging attack vector within the cyber security industry.[74] A 2022 report by cyber security firm Wallarm, found 18 high risk vulnerabilities in APIs which had been developed by large technology organisations including Veeam and Airspan.[75] These vulnerabilities included improper code controls allowing code injection, improper access controls, operation system misconfigurations allowing for command injections, and server-side request forgery. Many of these vulnerabilities were assessed at high to critical severity under the common vulnerability scoring system.

Salt Labs also found that in 2022 its clients have sustained a 117% increase in API attack traffic.[76] The extent of API compromises again Salt Lab's clients has led to 31% of these organisations experiencing a sensitive data exposure or privacy incident, and 15% being exposed to account misuse and fraud attempts.

Advanced Persistent Threats (**APT**) are commonly associated with nation states[77] and pose a significantly greater (if not the greatest) Threat to the CDR due to sophisticated levels of tradecraft, cyber capabilities and significant resources deployed with ATP's which will allow Nation State Actors to use multiple attack vectors (e.g., cyber, physical, and deception) over an extended period.[78]

According to the National Institute of Standards and Technology (**NIST**), APTs are a sophisticated Attacker who typically pursue their objectives repeatedly over a long period of time, are able to adapt to a defender's efforts to fend or resist its attack and are highly focused to maintain the level of engagement needed to achieve its objectives.[79]

APT attacks are often defined by common stages including infiltration, for example through a sophisticated social engineering campaign, escalation and lateral movement through the victim's network to map and gather credentials[80] High profile APT attacks include the 2016 compromise of the Hillary Clinton presidential campaign and the Democratic National Committee by APT28 (a Russian nation state APT from the GRU also known as Fancy Bear) to disrupt and interfere with the presidential election.[81] Then, in 2018, the US Department of Justice indicted five APT28 officers for long term, sophisticated attacks against significant targets, including the World Anti-Doping Agency, the US Anti-Doping Agency, a US nuclear facility, and the Organisation for the Prohibition of Chemical Weapons.[82] Another example of a Chinese nation state APT is the People's Liberation Army 61398. In 2014, the US Department of Justice indicted members of the unit for conducting a commercial cyber espionage campaign against various US companies including Westinghouse, Solar World and US Steel.[83]

Nation state attacks against Data Holders and ADRs are likely given these Attackers will see value in accessing CDR data and attempting to infiltrate the consumers and organisations connected to the CDR. Due to the sophisticated capabilities

of Nation State Actors, attacks can be launched across the entire CDR data lifecycle, and Threats may arise at any point where CDR data is stored, transferred or used by a CDR participant. Nation State Actors will have capabilities to bypass many standard cybersecurity controls, meaning few participants within the CDR will have sufficient cyber maturity to prevent compromises. Given the level of sophistication, early identification of potential incidents and effective recovery and resilience across all CDR participants must be prioritised to provide the most effective Threat mitigation outcomes.

New challenges will emerge with the expansion of the CDR and as different sectors are added to the CDR. This will create further motivation for Nation State Actors to attempt to attack and compromise CDR participants.

3.2 Cybercrime Groups

In the current digital landscape, a large volume of malicious cyberattacks are carried out by criminal enterprises.[84] A recent Australian Institute of Criminology Bulletin highlighted the scale of the problem citing a 2020 survey which found that 57 percent of Australian respondents reported having been a victim of cybercrime, with 33 percent having been victimised in the previous 12 months.[85] Recent reports have also estimated that more than half of Australian businesses have been disrupted by criminal cyberattacks over the previous 12 months.[86] Cybercriminal activity continues to include small scale and petty criminals, but increasingly it includes well-resourced Cybercrime Groups facilitated by the emergence of well organised marketplaces for stolen data on the Dark Web. Because of the size and value of their operations, CDR participants, and the CDR ecosystem as a whole, will be attractive to Organised Cybercrime Groups.

> The Dark Web has become a central pillar of the cybercriminal ecosystem, and a primary means for cybercriminals to resource and monetarise their activities. The Dark Web is an intentionally hidden part of the internet that cannot be accessed using regular web browsers or search engines. Generally, it consists of layers of encryption and hidden internet sites which can only be accessed through specialised browsers such as The Onion Router (Tor). The Dark Web has been designed to limit traceability, providing a higher level of anonymity for users. Numerous marketplaces and sites exist on the Dark Web, which allow Attackers to trade stolen datasets, sell compromised user credentials, procure malicious hacking tools, and to obtain resources to support cyber-attacks against organisations and individuals.

Typically, Cybercrime Groups can be divided into two discrete sub-categories: (1) Organised Cybercriminals and (2) Traditional Organised Crime Groups. Both sub-categories are considered below. These two categories are linked. The growth of Dark Web marketplaces has led to the rise of specialist brokers and facilitators that help to connect malicious actors with technical experts and resources across the cybercriminal ecosystem. Using these facilitators, criminal groups can grow their offensive capabilities, and directly engage parties who can support launching cyberattacks against target organisations. Brokers and facilitators can support a range of Crime-as-a-Service offerings for cybercriminals including Malware as a Service (**MaaS**), Ransomware as a Service (**RaaS**), toolkits licencing, affiliate models, automated phishing campaigns, and the provision of botnets to perform Distributed Denial of Service (**DDoS**) attacks. For more information on these, see Appendix

3.2.1 Organised Cybercriminals

As the CDR continues to evolve and allow for more complex consumer facing interactions and actions, this will create new Threats of harm and fraud against CDR participants. As Organised Cybercriminals become aware of the size and scale of the CDR, the likelihood of cyberattacks will increase. Large scale attacks against systems of significance such as the CDR are a relatively easy method for Organised Cybercriminals to commit large scale financially rewarding cyber operations, due to ease of purchasing attack tools and the repeatably of attack-chains. Data Holders and ADRs will experience cyberattacks of this nature from various Organised Cybercriminals.

Organised Cybercriminals are also building deliberate capabilities to commit mass-scale cyber operations and are becoming increasingly sophisticated enterprises, with many adopting structured organisation charts, designated leadership roles, finance departments, human resources, marketing, R&D, project managers, and outsourcing functions.[87]

Entities participating in the CDR ecosystem including Data Holders, ADRs and Trusted Advisers will face cyberattacks from various Organised Cybercriminals. There exist a number of well developed, resourced and established Organised Cybercriminals, for example:

- **Cobalt Cybercrime Gang** who historically targeted financial firms through spear-phishing emails that contained a malware attachment, ultimately allowing hackers to gain access to the internal network systems and to remotely control ATMs, disbursing money at specific locations where cybercriminals would wait and collect the money.[88]
- **MageCart group** is a well-known hacking Cybercrime Group that steals personal datasets from online websites using online skimming techniques to extract personal and financial information and datasets.[89]
- **Evil Corp** is a cybercriminal hacking group that steals user financial credentials using various variations of malware software to initiate phishing campaigns on unknowing victims; they then steal login details and gain access to their banking accounts.[90]

These cybercriminals operate worldwide conducting various cyberattacks against a broad range of organisations and institutions. In Australia, cybercriminals attacks are "prolific" causing widespread impacts across the Australian community.[91] Organised Cybercriminals will be the most active Threat Actors impacting the CDR, with ADRs and Data Holders finding themselves regularly targeted by these Actors. CDR participants will be continuously exposed to the most common attack methods used by cybercriminals, which are described in Appendix A.

Organised Cybercriminals will closely monitor the on-going rollout of the CDR and target entities which aggregate CDR datasets. These datasets could be used to facilitate a range of malicious attacks against CDR participants, particularly via social engineering attempts, ransomware attacks and identity fraud. Organised Cybercriminals regularly use stolen identities to commit fraud and target financial records, transactions history, personal information, marketplace data, client identifiers, bank account details, taxation returns, and healthcare information.

Organised Cybercriminals are likely to commit CDR focused API attacks and data scraping. API compromises by Organised Cybercriminals can blur the line between cyber security and traditional crimes. In a 2022 scraping incident, Ulta Beauty experienced a 700% surge in requests made against its local inventory search API. Subsequent investigations revealed that the Attacker had used proxy IP addresses to scrape data for 61,000 zip codes and 33,000 products.[92] Ulta Beauty sold a range of high-end personal care products that were in demand. Commentators found that the scraped data could have been used to identify the physical locations which stored the organisation's most valuable inventory. This data would provide important insights for criminals attempting to physically steal and re-sell Ulta Beauty's products.[93]

A key motive for cybercriminals is financial gain. As such, Organised Cybercriminals will be strongly motivated to steal CDR data which can be used to facilitate identity theft. Identity theft involves the use of stolen personal information to conduct fraudulent activities.[94] Organised Cybercriminals will leverage stolen identities to apply for loans or mortgages using victims' credentials and will target taxation returns, healthcare refunds, and online marketplaces and transaction data. Organised Cybercriminals also target driver licences, passports, Medicare cards and bank account details to facilitate fraudulent transactions.[95] Data Holders and ADRs will hold many forms of financial and transaction consumer data. This data will be valuable to Organised Cybercriminals attempting identity theft, making these CDR participants lucrative targets. Compromised CDR consumers that are exposed identity theft will experience financial and emotional consequences heightening consumer hesitancy with the CDR.

Further, Organised Cybercriminals will use extortion methods to demand ransom payments. Cybercriminals have now begun adopting double and triple extortion methods, under which impacted organisations are initially extorted to resolve the "availability" component of the attack, and then subsequently faced with a second extortion to prevent sensitive records being disclosed and published, and finally a third extortion where Threats are made directly against individuals whose sensitive data in compromised by the malicious intrusion.[96] Data Holders and ADRs will hold many forms of financial and transaction consumer data that will be valuable to criminal groups attempting to perform extortion demands. This will make CDR participants lucrative targets. Compromised CDR consumers will experience financial and emotional consequences and successful intrusions by Organised Cybercriminals will heighten consumer hesitancy with the CDR.

The overall security of the CDR and the ability of participants to prevent attacks by Organised Cybercriminals will require holistic strategies that align and enhance CDR Data Standards and accreditation processes and promote strong cybersecurity controls across Data Holders, ADRs, and Trusted Advisers that are permitted to store, transfer, and use CDR data. The Data Standards and accreditation processes require ADRs and Data Holders to have security processes in place including implementing steps to protect from data misuse, interference, loss, unauthorised access, modification, and disclosure.[97] Failure to maintain security controls will foreseeably result in unauthorised access of critical CDR datasets.

CDR data could be retained by criminal third parties for a significant period of time, resulting in potential long-tail exposures. Even if CDR data is exposed many years after a cyber incident, wider reputational harms will still exist for those affected and the regime as a whole. Organised Cybercriminals will intentionally harm individuals through misuse of transactional and payment data that create other avenues for victim exploitation. Even where credit card numbers or bank account details have been changed or are expired, an impacted individual's identity will continue to be impaired, because this data can be used to attempt future identity fraud and social engineering attacks. The range of data held by ADRs, Trusted Advisers and Data Holders is lucrative for identity fraud attempts as it may include rich personal information and transaction history details for a consumer. Where CDR data is exfiltrated, the CDR regime will face public scrutiny and consequential consumer distrust. This creates a complex and long-term Threat landscape that must be navigated in order to achieve the CDR's overall policy objectives.

Threats to the CDR by Organised Cybercriminals are likely to be immediate, as reports have identified the Finance and Technology sectors as amongst the most targeted industry sectors so far in 2022.[98]

3.2 Cybercrime Groups (continued)

3.2.2 Traditional Organised Crime Groups

Traditional Organised Crime Groups have a longstanding history of conducting crime, including illicit drug activities; financial crime; identity crime; money laundering; and humanitarian crimes.[99] Increasingly, technology is relied upon by Traditional Organised Crime Groups to perform their criminal actions, and more recently to extend their capabilities into cybercrime.[100] For example, allegedly a Russian organised crime syndicate is behind the selling of template scam scripts online together with fake call-centre support.[101] These well-established cybercriminal techniques[102] are increasingly being adopted by Traditional Organised Crime Groups.

While Traditional Organised Criminal Groups do not currently seem to possess high levels of technical expertise, they have a powerful ability to intimidate and coerce insiders which is often the key step in enabling a technology enabled attack. Increasingly, criminals who lack digital technical and offensive attack skills employ Organised Cybercriminals who can provide the required capabilities or software to execute cyberattacks. In a similar way it is possible that Traditional Organised Criminal Groups could provide specialist coercion and insider capability as part of a larger multi-party attack.

3.3 Competitive Intelligence Threat Actors

Competitive Intelligence Threat Actors are organisations that conduct cyberattacks against rival organisations with the objective of gaining a commercial or competitive advantage over the victim.[103] Within a cybersecurity context, this behaviour is most commonly seen when competitor organisations provide similar products or services and are able to derive similar financial and non-financial advantages from identical data sets.[104]

The CDR rightly promotes competition and competitive tension between participants. There is no doubt that the vast majority of CDR Actors will ethically and fairly approach competition within the CDR. The discussion in this section on Competitive Intelligence Threat Actors is by no means intended to suggest these Threat Actors will be prolific, however there are numerous global examples which must be managed within the context of the CDR's data security environment.

The range of potential motivations for Competitive Intelligence Threat Actors can be seen in cases such as *United States v. Ticketmaster Entertainment, Inc., et al*,[105] where unauthorised data extracted from a competitor was used by the defendants to (among other things) prepare strategy presentations, benchmark competitor products and services, devise new client facing services, identify potential customer segments, and build better relationships with third parties.

CDR participants will hold data attractive to Competitive Intelligence Threat Actors including personal user and contact information, sensitive datasets on individual preferences and service requirements, sensitive product data, operational data, and intellectual property.[106] Many of these data sets will be intermingled within the underlying Data Holder's system and may be commonly exposed in a successful cyber intrusion. Where intermingled data is compromised this will increase the potential harm a Competitive Intelligence Threat Actor could inflict on the victim and the CDR.

As a general group, Competitive Intelligence Threat Actors tend to be well-resourced, deploying strategic and targeted cyberattacks[107] with the intention of obtaining unauthorised access to competitor data assets and extracting relevant data from competitors. Beyond data exfiltration and unauthorised use of CDR data, significant reputational harm is likely to result for the compromised CDR participant. Using recent major Australian data breaches as a guide, the harm consequences for CDR participants compromised by Competitive Intelligence Threat Actors will include public and stakeholder criticism, client churn and suspensions, trading losses, and legal and commercial exposures.[108]

The heightened competition promoted by the CDR increases the likelihood of competitive intelligence behaviour because many Data Holders, ADRs and Trusted Advisers within the CDR regime will be direct competitors. While it is anticipated most will adopt proper practices, CDR participants may see tactical and financial advantages in compromising and disrupting rival CDR participants' services.

Competitive Intelligence Threat Actors will be motivated to commit unauthorised data scraping attacks, as they facilitate accumulation and warehousing of valuable data assets and provide unfair advantages over rival firms, who are limited to the lawful and authorised data collection behaviour.[109] The recent US Eleventh Circuit Court Decision of *Compulife Software Inc. v. Newman*[110] provides an example of how data scraping between CDR participants could occur. In *Compulife Software Inc. v. Newman*, the plaintiff and defendant were direct competitors that generated life insurance quotes. It was alleged that the defendant had hired a third party to use scraping techniques to create a partial copy of the plaintiff's database and to extract insurance quote data. The extracted data allowed the defendant to analyse the plaintiff's insurance quote data and build a rival quote engine. This involved extracting and saving all the premium estimates for every possible combination of demographic data within those two zip codes, totalling more than 43 million quotes.

In a similar vein, it has also been alleged by a former employee that Uber's internal 'Intelligence Team' regularly impersonated riders and drivers on rivals' platforms and then attempted to hack into their rivals' systems to learn about their key processes, identify security loopholes in rivals applications, and harvest data on drivers and users.[111] These allegations were contained in the 2017 'Jacob's Letter' which identified that competitive intelligence hacking and surveillance behaviour formed part of Uber's wider tactic to 'gain an edge over' all of its competition.[112]

As seen in *Compulife v Newman*, competitive intelligence cyber events commonly result in allegations of substantive civil law breaches including of copyright law, trade secrets and contract law, in addition to criminal liability attaching to the Attacker. Civil legal and regulatory contraventions can also arise for the victim organisation where unauthorised access and loss of data occurs.[113] In the case of the CDR, if Data Holders and ADRs are subject to competitive intelligence cyberattacks, they are likely to face conventions of privacy laws and the CCA,[114] contractual confidentiality provisions, service and performance agreements[115] and civil liability from impacted individuals arising from the unauthorised access to CDR data and associated information assets.[116]

Competitive intelligence cyber events may also cause reputational damage to the CDR where exfiltrated data, originally

3.3 Competitive Intelligence Threat Actors (continued)

in the custody of an ADRs or a Data Holder, is incorrectly used by the Threat Actor. The scope of CDR data will regularly include significant financial information, such as an individual's transactions and interaction data with the Data Holder, payment information, credit records, and information on an individual's personal and financial circumstances. Threat Actors that leverage this data without consent or consumer authority may threaten the integrity of the CDR. A Competitive Intelligence Threat Actor's motives may extend beyond extracting CDR data and involve impact to the technical components of a competitors' IT environment.[117]

As new participants in less regulated industries are added to the CDR, Competitive Intelligence Threat Actors may also be motivated to commit DDoS attacks.[118] DDoS cyber-attacks specifically threaten the operations of Data Holders and ADRs by rendering their internet-facing systems inoperable.[119] The inherent nature and interconnectivity of the CDR makes participants susceptible to widespread DDoS attacks which may stretch to all CDR participants and threaten availability to critical CDR reliant systems. The Amazon Web Services DDoS attack in 2020 demonstrates the sheer scale and impact of DDoS attacks; this resulted in an AWS 'elevated threat status' for three days.[120] DDoS Threats should be considered with the context of the recommended Data Standards Safety System. While it is not possible for the Chair to prevent the occurrence of a DDoS attack against a CDR participant, impacts resulting from a significant DDOS incident will undermine the availability of the CDR and overall public confidence in the CDR.

3.4 Trusted Insiders

Trusted Insiders refer to an organisation's internal members and trusted third parties whose conduct is directly attributable to data security incidents.[121] Individuals who make up this Threat Actor group typically include an organisation's current and former employees, independent contractors, professional advisers and key service providers.[122] Trusted Insiders cause cyber Threats through actions ranging from intentional malicious behaviour and through negligent conduct which is subsequently exploited in cyberattack chains. McKinsey & Company has found that many organisations are least prepared to confront Trusted Insider cyber Threats and that almost 50 percent of reported breaches can have a substantial 'insider' component.[123]

CDR participants constantly interact with and are exposed to Trusted Insiders. This is particularly so with Data Holders and ADRs who will have employees, contractors, and associates holding elevated privileges[124] within the organisation's IT environments. Insiders can directly access CDR data, operational network configurations, data security controls, intellectual property, and CDR operational data. These arrangements create direct opportunities for Attackers.

Although the Chair cannot prevent malicious Trusted Insiders, it is important these Threat Actors are considered when modelling Threats due to their potential ability to circumvent security controls and the consequent widespread impacts their actions may cause. In addition to common cyberattacks described in Appendix A, Trusted Insiders may also inject malicious code into services that sit across the CDR ecosystem, delete or exfiltrate CDR data, compromise encryption keys, and facilitate the malicious actions of other Attackers. Trusted Insider Threats are however diverse, and within CDR can arise in all circumstance where data it is being used for CDR related purposes. For these reasons, it is important Trusted Insider Threats are carefully analysed within the context of the Data Standards and CDR data security generally.

Trusted Insiders will typically include three distinct sub-categories of Threat Actors being:[125]

- malicious staff;
- compromised staff; and
- innocent or careless staff.

3.4.1 Malicious Staff

There is strong overlap between the motivations of malicious staff and the motivation of Competitive Intelligence Threat Actors, discussed above. Malicious staff may also be influenced by emotional drivers,[126] diverse financial goals, and political agendas[127] as was seen in the 2019 Capital One Data Breach. In this incident, the convicted hacker was a former Amazon Web Service employee who continued to have access to Capital One's cloud data repositories after their employment was terminated.[128] The prosecution alleged the hacker committed the cyberattack to mine cryptocurrency leveraging Capital One's IT systems, to access and exfiltrate Capital One's client data, to extort Capital One and to brag of the successful intrusion to their peers.[129] The hacker's direct knowledge of Capital One's infrastructure allowed them to utilise a misconfigured firewall to access credentials and consumer data.[130]

Similar malicious staff actions may be committed by employees of CDR participants to what was seen in 2019 when a malicious employee of the Canadian financial institution Desjardins used both their privileged access and several colleagues authentication credentials to access and collate personal and corporate information for 4.2 million individuals and 173,000 businesses.[131] The employee reportedly stole data including names, addresses, date of birth, government identification numbers and customer behaviour information.[132] Many Data Holders within the CDR will hold similarly diverse and rich consumers data assets, that will attract the attention of malicious staff.

Some malicious staff will also be financially motivated to warehouse and on-sell CDR data to cybercriminals, as was seen when a malicious insider extracted 2 million consumer email address from OpenSea, a nonfungible token marketplace.[133] It has been alleged that these records were of particular value to cybercriminals, who could then deploy phishing attacks against OpenSea's users in an attempt to steal the users' nonfungible tokens.[134] CDR participants hold extensive consumer datasets and information that Attackers could use to undertake social engineering attacks against CDR consumers.

Malicious staff can also cause widespread harm to a CDR participants' business reputation and financial operations by exposing critical data or compromising intellectual property. In 2016, it was alleged an employee of Waymo (formerly the self-driving car unit at Google) stole more than 14,000 files from its system, including trade secrets and LiDAR technology,[135] with the intention of starting a new company to be incorporated within a competitor.[136]

3.4 Trusted Insiders (continued)

Automation, outsourcing arrangements, and the reliance CDR participants place on Trusted Advisers will also create malicious staff Threats. In 2017, Anthem BlueCross BlueShield (**Anthem**) had 18,500 consumer records exfiltrated[137] due to an engaged vendor's malicious employee.[138] This followed an earlier 2015 Anthem cyber incident.[139] Despite performing investigation and cybersecurity uplift work between 2015 and 2017, Anthem was not able to prevent the 2017 cyber incident, demonstrating how difficult it is for organisations of all sizes to protect their data from third party malicious staff.[140] Where the Data Standards and other CDR mechanisms can be expanded to consider these issues, it will enhance overall security and confidence within the CDR.

3.4.2 Compromised Staff

Compromised staff are those users who have been coerced or tricked into providing a third party with sensitive or business critical data,[141] often by means of social engineering.[142] Irrespective of the method, a compromised user becomes a component in the 'attack chain' of a malicious cyber intrusion against the target organisation. Many compromised staff do not have malicious intentions[143] though they may be an element of recklessness in their conduct, as was seen in July 2020, when a group of hackers coerced an internal Twitter employee into providing credentials for the organisation's administrative tools.[144] Despite the compromised user within Twitter having no desire to cause damage, significant harm followed as the tools facilitated Twitter account takeovers, which allowed third party hackers caused hundreds of thousands of dollars to be stolen and resulted in widespread reputational damage.[145] Compromised staff can also cause cyber incidents where an employee device has been infected with malicious software, providing a staging point for future attacks.[146]

It is unavoidable that at least some Threats arising from compromised staff will exist within the CDR's ecosystem, and that actions involving compromised staff will form part of the social engineering, staging and coercion activities undertaken by cyber Threat Actors.[147] While the Data Standards cannot directly mitigate the risk of compromised staff Threats, there is benefit in considering the availability of compensating controls and process to ensure CDR data is stored, transferred and used in ways which are consistent with the CDR's overall objectives.

3.4.3 Careless Staff

In contrast to compromised or malicious staff, careless staff perpetrate cyber incidents through acts or errors which cause '*unintended results*'.[148] Some examples of careless behaviours include violations of an organisation's security policies, undermining cybersecurity controls, and activities which expose an organisation to outside harm.[149] The Threats posed by careless staff are closely related to the human elements of cybersecurity.[150]

One of the most common forms of careless staff Threats is inadvertent disclosure by an employee or third party of sensitive information to an incorrect recipient. In its July to December 2021 Notifiable Data Breaches Report, the OAIC found that 21% of all reported data breach incidents involved the unintended release or publication of personal information.[151] Cybersecurity events of this nature may be particularly damaging to the CDR and CDR participants, where they directly undermine the consumer consent and authorisation protections contained within the CCA, CDR Rules, and Data Standards.

3.5 Hacktivists

Hacktivist Threat Actors differ from the other Threat Actor groups as they are motivated by injustice and ideology rather than financial gain or intelligence gathering agendas.[152] These Threat Actors comprise of disparate individuals who seek to compromise technology environments to carry out political, social or religious activism to initiate their desired change.[153]

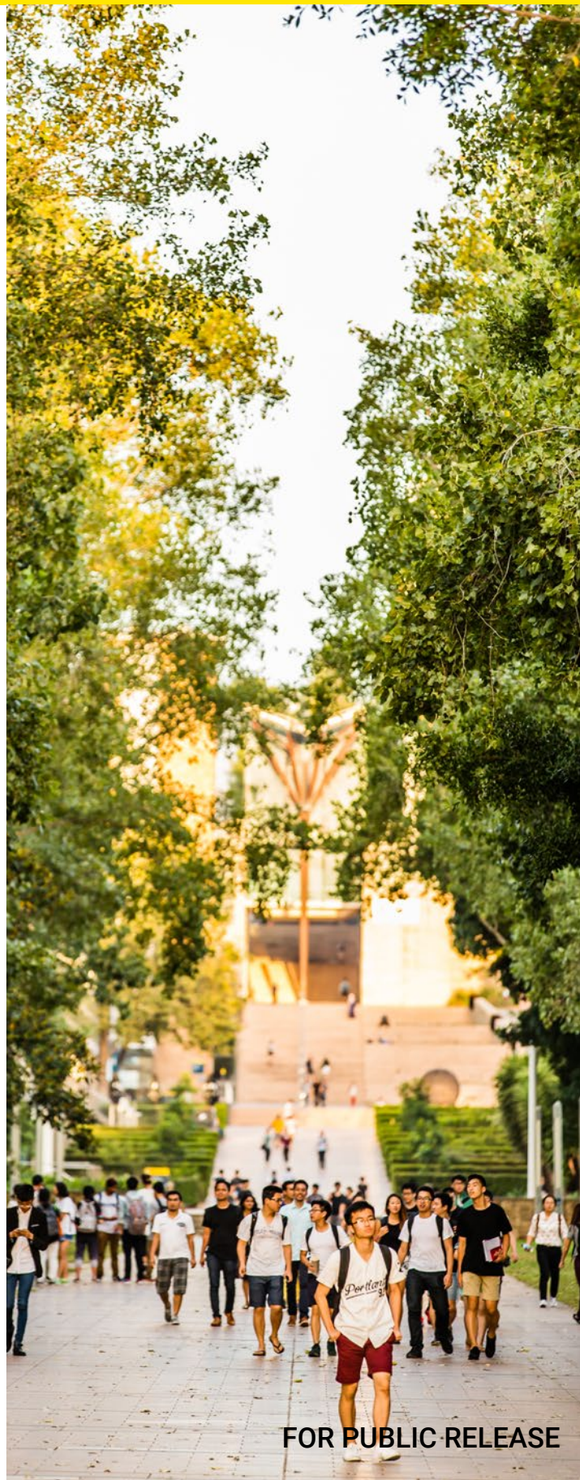
The Threat posed by Hacktivists is frequently discounted as they are often categorised as 'juvenile script kiddies',[154] implying that they are unskilled amateur hackers who use existing paid or pre-developed software, programs or services to initiate an attack.[155] In a world of increasing geopolitical tensions, Hacktivist cyberattacks are increasing in sophistication and regularly target Government agencies and departments, multinational corporations and high-profile individuals and can deploy well thought-out strategic cyberattacks.

The 'Anonymous Group' is a well-known Hacktivist group that has initiated multiple cyberattacks to promote social and political issues. Recently, Anonymous attacked the Russian Central Bank, where 28GB of data was publicly released in retaliation to the ongoing Russia-Ukraine conflict.[156] Another recent Hacktivist initiated cyberattack was on the Minneapolis Police Department in support of the Black Lives Matter movement, where hackers launched DDoS attacks on the department rendering a number of services inoperable.[157]

In June 2022, three large steel companies in Iran were subject to cyberattacks by Hacktivists who posted and took responsibility for the attack on social media sites.[158] The cyberattack reportedly caused machinery to 'malfunction' and caused a 'massive fire'. The hackers justified their actions on the basis that the entities were operating in restricted international sanctioned areas.[159]

These attacks demonstrate the diverse nature and degree of capability that Hacktivist groups now have. They illustrate how CDR participants may find themselves collateral damage of a Hacktivist attack on a related entity, or that CDR participants could be a direct target where Hacktivists see benefit in disrupting their services or to further the Hacktivist's specific message.

The CDR regime will continue to expand across the critical sectors of Australian society and infrastructure. It is reasonable to expect that some Data Holders, Trusted Advisers and ADRs will be directly targeted or experience collateral damage from Hacktivists, where their operational activities or social governance do not align with Hacktivists' social and political ideas.



3.6 Conclusion

This section has discussed the landscape of current Threat Actors that could impact the CDR. Given the pace of technological advances and range of malicious parties targeting the CDR, the Chair will need to be mindful of the following Threat landscape issues within the context of their statutory powers and functions:

- Large scale attacks against systems of significance, such as CDR, will be attempted by many Threat Actors particularly APTs such as Nation State Actors and Organised Cybercriminals;
- APIs are foreshadowed to become a significant target for Threat Actors. Threat Actors will target API data security across the CDR and the areas most exposed are in the transport, authentication, insecure coding, and input validation of the API requests.
- Data security across the CDR will be influenced by the data handling behaviours of CDR participants throughout the entire data lifecycle. Many organisations are pursuing additional insights from data using artificial intelligence. Each of these derivative data processes, and any parties that CDR data is shared with, will create potential new means for Threats against the CDR. This is one example of dynamic emerging Threats that must be continually monitored and assessed in order to maintain confidence in the overall data security state of the CDR.
- As less mature organisations begin to enter the CDR ecosystem, new security Threats will transpire for all parties involved. One challenge that must be managed is the security controls and culture that smaller, less cyber mature entities will have, or rather the potential that they will have limited security and Threat management capabilities.
- The frequency of cyberattacks is increasing at a rapid rate and is outpacing the ability to upskill and hire cybersecurity resources. The potential inability of CDR participants to employ security personnel to effectively monitor security systems and controls could impact the CDR's reputation and consumer confidence where a data breach eventuates. This will be particularly felt when a breached entity could have reduced a Threat through analyst monitoring, or effective security control configuration.
- API security is likely to pose challenges from numerous Data Holders, ADRs and other parties in the CDR ecosystem. A number of parties will struggle to understand their APIs and their purpose within the environment. Complexities will also arise where the product and services developed by CDR participants rely on multiple APIs or where APIs are not fully supported within an organisation.

4. How to Approach Threat Modelling

4.1. A Structured Approach to Threat Modelling

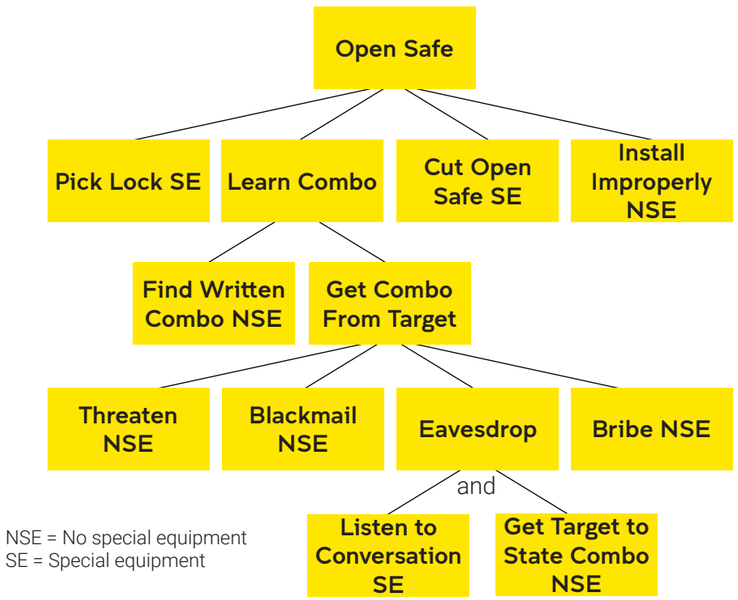
This section introduces our recommended approach to Threat Modelling. It is important to note that the approach we describe is not a once-only activity. Whilst there are multiple paradigms for conducting Threat Modelling, a Threat Model once built is not static – it needs to be a live document and updated in response to changes in the system, the Threat landscape, and external factors. This must involve both regular formal reviews, supported by ongoing continuous monitoring and consideration of Threat. Internal and environmental changes bring with them the possibility of new Threat scenarios and attacks and/or a weakening of the effectiveness of the currently adopted security controls. It is important to continuously track those changes and what new attacks they allow for on new and existing system components. This section outlines industry best-practice as it applies to this space.

4.1. A Structured Approach to Threat Modelling

Threat Modelling is a *structured* approach undertaken by defenders to ensure that as many as possible of the potential Threats to the assets of a system are anticipated and considered in advance. Threat Modelling is widely used across many industries, both for newly developed software and for the ongoing deployment of existing systems.

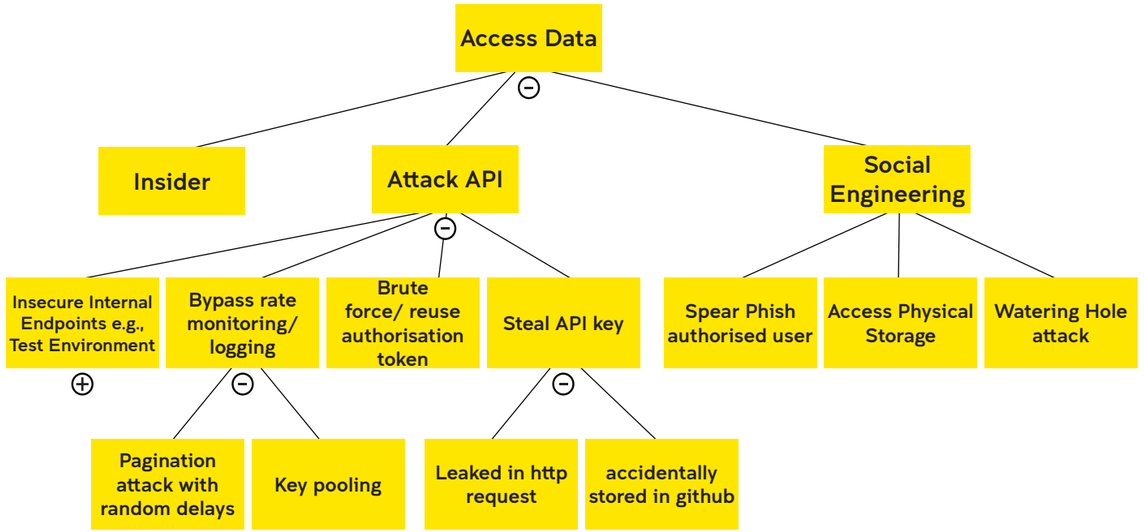
Pursuing a structured approach provides several advantages. Identifying and enumerating the potential Threats to a system *could* be done in an unstructured manner by well informed and experienced defenders with a good knowledge of the system. Indeed, historically this was often the approach taken. However, when systems are complex, and Attackers are motivated, and attacks on the system could have significant consequences, an unstructured approach is fraught with unnecessary risk. In particular, a structured approach to Threat Modelling helps ensure that defenders do not inadvertently overlook some significant Threats in their security planning. This is important for two reasons. It is likely that Threat Actors, particularly the more sophisticated ones such as Nation State Actors and Cybercrime Groups, given sufficient time and motivation, will discover any overlooked gaps. Second, security is asymmetric – successful Threat Actors need only find one vulnerable point whereas successful defenders need to defend all points.

A structured approach is central to the Threat Modelling methodologies and frameworks that have been developed and evolved over time. Early simple structured approaches include Attack Trees (also called Threat Trees) which were devised by renowned security expert Bruce Schneier in 1999 whereby attacks are successively broken into more detailed sub-attacks and depicted as a structured tree diagram. Schneier gave the example of an Attacker with goal of opening a safe:[160]



4.1 A Structured Approach to Threat Modelling (continued)

A simplified example Attack Tree for stealing data from a target is given below as a further illustration of the use of a structured approach in modelling:



More recent Threat Modelling methodologies and frameworks from OWASP, Octave, STRIDE, and Mitre use more elaborate structured approaches to develop a more comprehensive understanding of the Threats to a system, including various ways of understanding the nature of the system, ways of classifying and breaking down sources of Threats, ways of enumerating the assets which need to be protected, and so forth.

Although modern Threat Modelling approaches differ in the details, they all serve the same purpose of providing a systematic structured process for security planners to follow to facilitate, and so support, the planners to notice and investigate as many potential Threats as possible.

Developing an understanding of Threat for the CDR involves developing a holistic understanding of the entire CDR ecosystem and taking a security engineering and Attacker perspective to notice possible attacks and weaknesses. In essence, what are the key components of the system, and for each of these, what are all the things that could go wrong, be worked around, bypassed, exploited, leaked, or destroyed?[161]

It is important to note when reading this section that most Threat Modelling methodologies also involve further steps that are outside of the scope of this Report. The purpose of modern Threat Modelling is to identify malicious or accidental Threats in the system, and then to plan Threat countermeasures (**controls**) and develop protective sub-systems with the overall goal of preventing or mitigating the damage of each Threat event. The scope of this Report is to consider Threat Modelling as a way of identifying and assessing Threats, but not to consider the subsequent development of controls. Control frameworks form part of an overall RMF. However, carrying out those further steps would be consistent with and supported by the Threat Modelling methodology recommended here.

The wide range of Threat Modelling methodologies currently available[162] vary in their effectiveness at systematically identifying Threats and generating a sufficiently comprehensive Threat Model. More comprehensive Threat Models contain a summary of the system's major components, make explicit the assumptions made about the system, the categories of Threats to it, the specific Threats discovered in those categories, how to mitigate those Threats through controls and, most importantly, which methods to use to verify that those controls are sufficiently comprehensive so that the security solution works.

4.2 The Role of Threat Modelling in Government Risk Management Policies

In this section, we explain how government policy in relation to risk helps shape the way in which Threat Modelling should be conducted. There is guidance on the role of and method for Threat assessment in the contexts of the Commonwealth Risk Management Policy (**Risk Policy**), the Protective Security Policy Framework (**PSPF**) and relevant Australian standards.

4.2.1 Threat Modelling in Risk Policy

It would be impossible to build an RMF that met the requirements of the Risk Policy without a comprehensive identification and understanding of the Threats. This is because Threats and risks are tightly coupled, as Threats are the sources of risk.

For example, it is a requirement to have an RMF that supports the development of a positive risk culture by involving both Threats and opportunities in the identification, assessment, communication and management of risk.[163] Further, Element Seven requires each entity to "implement arrangements to understand and contribute to the management of shared risks".[164] Those responsible for aspect of the Risk Policy (because they have been allocated that responsibility under Risk Policy Element Three) must implement arrangements to understand risks that extend beyond the entity itself.

The relationship between the requirements in the Risk Policy and identification and assessment of Threats requires an understanding of both concepts. Risk is defined in the Risk Policy as the impact of uncertainty on objectives and is commonly expressed as a combination of consequences and likelihood of occurrence of an event. Risk identification is the process of finding, recognising and describing risks whereas Threats are the contributing causal factors for risks, and so increase the likelihood of negative events (such as data loss, system outage, unauthorised data transfer) that result in loss, damage or destruction of assets which, if they occurred, would be a "risk event". In the context of shared risk, these assets would include the benefits to multiple stakeholders associated with the CDR as well as assets associated with specific stakeholders such as consumers' privacy. The Risk Policy thus requires identification of Threats not just to the assets of the entity itself, but with an eye to the impact on the system's stakeholders more broadly. As has been stated in guidance material on the Risk Policy, "shared risk is a crucial element of program/policy delivery and failing to identify and manage these risks often impacts a broad range of stakeholders."[165]

Threat Modelling is best conducted as part of the process of identifying and analysing risk under the Risk Policy and PSPF. The guidance to implementing Element Seven of the Risk Policy provides further advice relevant to the conduct of Threat Modelling:

- **Documentation:** This aids in "understanding the complex relationships and clarifies the extent of knowledge of shared risks at a point in time".
- **Collaborate with stakeholders:** "Proactive and comprehensive information exchange is essential to fully identify the nature and severity of risks, monitor their status and manage the potential realisation of risks." Collaboration in the context of Threat Modelling can ensure that the "quality and availability of information on risk" is accurate.

Another mandatory requirement is Risk Policy Element Nine requiring review of risks. The risk assessment (including an understanding of Threats) thus must not be 'set and forget'. The guidance in relation to this element explains that risks change over time and that new risks need to be identified. Some new risks can be identified through 'near miss' and incident reporting (one of the practical tips offered in the guideline) while others will require broader situational awareness. On the latter, the guideline suggests that entities "consider a range of information sources".

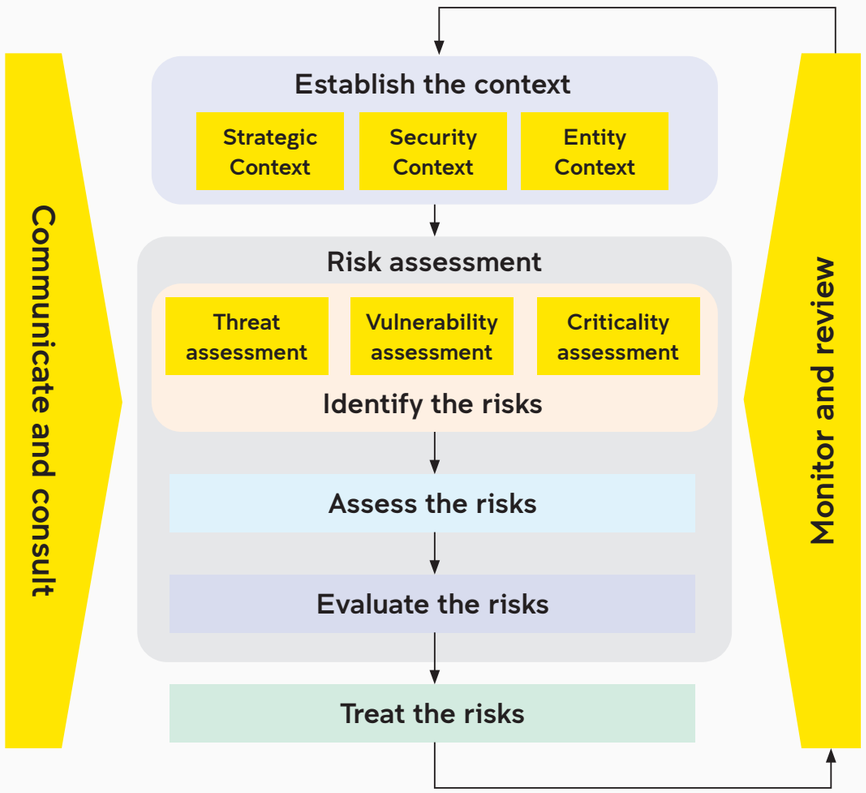
4.2 The Role of Threat Modelling in Government Risk Management Policies (continued)

4.2.2 Threat Assessment from PSPF Policy 3

The role of Threat assessment in the broader security risk management process is explained in Annex A to PSPF Policy 3 (Figure 2):

Figure 2

Protective Security Policy Framework
Annex A. Security risk management process
Annex A Figure 1 security risk management process



1. Elements of this guidance are based on the recommended Australian Standards: Commonwealth Risk Management Policy, AS/NZS ISO 31000 and HB 167 – Security Risk Management.
2. Risk is defined as the effect of uncertainty on objectives. An effect is a deviation from the expected – positive or negative4

Threat assessment comes after establishing the strategic, security and entity contexts and is one of three activities required to "identify the risk". The link between the three is explained in the Annex: "[Identifying security risks] is achieved by mapping the sources of risk (threat assessment), determining the importance of organisational assets (criticality of assets) and the manner in which these elements may facilitate or inhibit this interaction (vulnerability)." The Threat assessment itself "identifies the source of harm and is used to inform the entity's risk assessment. Threats are assessed by determining the intent to cause harm, damage or disruption and the capability (the potential that exists to cause harm or carry out intentions) of the threat source." Threat assessment in this sense is part of the Threat Modelling methodology recommended in this Report.

The Annex also includes a list of questions for the overall 'identify the risks' step:

- What could happen? (potential event or incident and resulting outcomes or consequences)
- What is the likely outcome and impact of the risk eventuating?
- When could it happen? (how frequently)
- Where could it happen? (physical location and assets affected)
- How could it happen? (sources, potential threats, catalysts, triggers)
- How reliable is the information that the risk assessment is based upon?
- Why could it happen? (causes, underlying factors, vulnerabilities or inadequacies in protective security controls or mitigations)
- Who could be involved or affected? (individuals or groups, stakeholders or service providers)
- Do entity mitigation measures or activities create risk to clients or the public?

There are also supporting requirements that are similarly mandatory including a requirement to review the security plan at least every two years; the guidance would suggest that processes be in place to identify changes in the Threat environment more generally and thus treat the security plan as a 'living' document. Further, it is a requirement to determine business impact levels for consequences of Threat and measure increases or decreases in risk as a consequence of a change in Threat to the entity (see Appendix D). The guidance explains this in terms of a "security alert level", which may change based on changes in (relevant) national terrorism Threat level, protective security risk reviews, police advice, emergency management advice, entity security incident reports and media reports. The centrality of Threat assessment in the formulation of a security plan is clear: "Successfully managing entity security risks and protecting people, information and assets requires an understanding of what needs protecting, what the Threat is and how assets will be protected."[166] The guidance suggests different sections of a security plan including a section on "security risk environment" that sets out the Threats, risks and vulnerabilities affecting the entity's protection, including, inter alia, "what it needs to protect against (via threat assessment)". There is other guidance offered for security plans including in relation to consultation.[167]

4.2.3 Threat Modelling from PSPF Policy 11

PSPF Policy 11 has as its core requirement ensuring the secure operation of the Commonwealth entity's own ICT systems to safeguard the continuous delivery of government business by applying the ISM's cybersecurity principles during all stages of the lifecycle of each system. This requirement applies to the ACCC with respect to, inter alia, systems used to maintain the Register of Accredited Persons. However, it does not apply directly to a government entity setting standards for the operation of third-party systems. Despite that, it is the considered advice of the ACSC, and should be taken into account in the context of the impact of consumer data standards on other entity's ICT systems. This would promote the holistic operation of government policy in the context of ICT security.

PSPF Policy 11 points to the ISM. The ISM includes guidance on application development.[168] That suggests specifically (Security Control ISM-1238; Rev 4; Applicability: All; Essential Eight: N/A) that "Threat Modelling is used in application development". This guidance applies to all entities building APIs within the CDR ecosystem. It does not apply directly to entities setting standards for others to build applications (such as the Chair). However, given that the government encourages organisations generally to comply with the ISM, it would be odd if the Chair were to require other organisations to develop applications in a particular way (in accordance with binding Data Standards) in the absence of such Threat Modelling having been conducted. Thus, Threat Modelling that aligns with the security control in the ISM in accordance with PSPF Policy 11, while not mandatory, would support broader government policy around cybersecurity. It is worth noting that the ISM includes a reference to OWASP as a security control relating specifically to the development of web applications. The ISM also includes guidance on cryptography and data transfers (inter alia).

4.2 The Role of Threat Modelling in Government Risk Management Policies (continued)

4.2.4 Threat Assessment from Standards Australia

AS/NZS ISO/IEC 27005:2012 is an international standard on security risk management for organisations. The standard is part of the ISO/IEC 27000 series dealing with information technology security techniques. It broadly aligns with the high-level risk management process specified in ISO 31000. The UNSW Risk Report identifies AS/NZS ISO/IEC 27005:2012 as a methodology to incorporate in developing an RMF for Data Standards. Identification of Threats is a component of risk identification. Annex C in the Standard gives examples of typical Threats, which may be useful to consider in Threat Modelling.

HB 167:2006, a local Australian and NZ standard on security risk management, underlies the approach taken in PSPF Policy 3 (which is mandatory) but provides more detail, particularly on Threat assessment. HB 167 emphasises the importance of understanding context as well as the root causes and drivers that feed into the beliefs, behaviours and structures that become Threats. It describes how to identify data and information sources (4.2) and sets out the purpose and process for criticality, Threat and vulnerability assessment. The Threat assessment component is at 4.4 with the method recognising the need to integrate two goals - (1) creative thinking about Threats and not being bound to a list as opposed to (2) the limits of time that require a focus on plausible scenarios. In developing a Threat Modelling framework, it is thus worth considering the lists, tables and worksheets in HB 167, while not being limited to those elements particularly in the context of newer emerging Threats. Note that HB 167 is broadly consistent with AS/NZS ISO 31000: 2009 on Risk Management – Principles and Guidelines and AS/NZS ISO/IEC 27005:2012 (described above).

A04:2001 is a new Australian standard on Insecure Design, which focuses on risks related to design flaws. It calls for use of Threat Modelling, secure design patterns and principles, and reference architectures.

A more extended list of relevant international and national standards relevant to risk management, security risk management and information security is set out in Section 4.1.5 of the UNSW Risk Report.

4.2.5 Summary of Threat Modelling Requirements for the Data Standards

This section has discussed how Threat Modelling can align with the Risk Policy, the PSPF and the most relevant Australian standards. While not all elements of these are mandatory - the Risk Policy is mandatory, the applicability of the PSPF to Data Standards implemented on non-government systems is variable, and compliance with Australian standards is encouraged – it is advisable to conduct Threat Modelling in line with all of these best practice statements unless there are reasons not to. Ultimately, given the embeddedness of these documents in government security policy more broadly, divergence should be both noted and justified. For example, the relationship between PSPF Policy 3 and the Data Standards which are implemented by CDR participants is best understood if one treats the CDR itself as an 'asset' and recognises that risks related to the CDR and, in particular, Data Standards, are shared with other agencies and participants in the CDR ecosystem. This might be done where, for example, a particular process is not, in fact, best practice or is not appropriate to the context.

The CDR Threat Modelling should:

- contribute to the development of an RMF through an understanding of Threats to the CDR ecosystem, in particular those that compromise the confidentiality, integrity and availability of CDR data throughout its lifetime as it moves through that ecosystem in line with the Data Standards;
- be based on an understanding of the context in which the Data Standards operate as well as the root causes and drivers that feed into the beliefs, behaviours and structures that become Threats;
- involve proactive and comprehensive information exchange with stakeholders to ensure the quality and availability of information on Threats, particularly in the context of Threats that result in negative consequences to stakeholders as well as to the CDR itself and the wider digital economy;
- be documented to aid in genuine understanding not only within DSB but also for impacted stakeholders with varying levels of cybersecurity maturity and background;
- be conducted continuously over the life of the CDR, supplemented by formal reviews at least every two years and more frequently as warranted, for example when there are significant changes in the Threat environment or CDR scope (including as part of any post-incident response, known near misses or changes in the risk context e.g. national terrorism Threat levels) and treated as a living document.
- be done during the planning phase before implementing changes in CDR scope or functionality.[169]

The Threat Modelling should, together with vulnerability and criticality assessment, contribute to answering the questions set out in PSPF Policy 3 (which uses the related term Threat Assessment). In particular, the Threat Modelling should lay out what could happen, when and where it could happen, how it could happen, why it could happen, who could be involved or affected and the reliability of information sources used in the analysis.

Note that although the lowest acceptable frequency for formal security reviews under these policies when situations are stable is once every second year we expect that in practice CDR formal reviews including Threat Modelling will likely be carried out annually given the ongoing and anticipated rates of change experienced by the CDR including additional functionality, additional industries being brought into the scheme, and projected increases in the volume of consumer data being protected.

As mentioned in Section 1.2.4, the Threat Modelling should also be guided by HB 167:2006. The lists, tables and worksheets in that standard can be integrated into the framework used for Threat Modelling, to the extent they are useful and appropriate.

OWASP (The Open Web Application Security Project) is referenced in the ISM, particularly in the context of web applications.[170] While it does not directly apply to *standards for* web applications, its use is encouraged. OWASP Threat Modelling recommendations include guidance[171] on Threat Modelling and a Threat Modelling Process "OWASP-TMP"[172] incorporating the STRIDE Threat categories. Both the OWASP-TMP Threat Modelling methodology and the STRIDE Threat Modelling framework are discussed in more detail in Sections 4.3-4.5.

4.3 Recommended Threat Modelling Approach for Data Standards

After consideration of the range of established Threat Modelling methodologies and frameworks from the perspective of the Data Standards, we recommend a synthesised approach as being most appropriate for the purposes of the Chair. In particular, we recommend that OWASP-TMP be adopted as the Threat Modelling process for the Data Standards, and that the STRIDE Threat classification framework be used in the Threat identification stage of that process.

We make this recommendation for the following reasons:

- Both are widely adopted and used by threat modellers in practice so there will be sufficient capability to carry out the process available to the Chair.
- This approach is well supported by online documentation, resources, and tools.
- This approach is capable of generating a comprehensive coverage of the Threats to consumer data and to the aspects of the CDR which are the responsibility of the Chair.
- The same Threat Modelling process can be used across the full CDR ecosystem by participants and governance bodies with security responsibilities should they choose to do so. Were this to happen, the various outputs and findings could be conveniently integrated. This would support a holistic approach to cybersecurity across the whole of the CDR ecosystem. As previously discussed, the security of the CDR as a whole is better served by a single view of security planning across the whole ecosystem that is supported by all participants. That is clearly preferable to a collection of fragmented security planning activities carried out by the various entities individually and in isolation.
- The process and outputs of the OWASP-TMP Threat Modelling methodology will conveniently extend to integrate the Threat Modelling process with the subsequent risk quantification and selection of security controls carried out under the overall RMF.
- OWASP-TMP and STRIDE are well supported and referenced in existing security modelling activities carried out across government.
- The Threat types considered in the STRIDE categorisation framework align with the main likely categories of Threats to the consumer data as well as to the CDR more generally – namely Authentication (**S**poofing), Integrity (**T**ampering), Non-repudiation (**R**epudiation), Confidentiality and Privacy (**I**nformation disclosure), Availability (**D**enial of Service), and Authorisation (**E**levation of Privilege).
- The OWASP-TMP modelling methodology is focussed on a genuine and collaborative approach to Threat identification as part of the mindset to be adopted. With all Threat Modelling frameworks, it is possible to carry them out poorly or in a tokenistic way, appearing to comply on the surface but not accomplishing much in practice. Identifying the full set of relevant Threats which need to be considered requires not only a structured approach, but also determination and collaboration. The OWASP-TMP methodology has a strong focus on values and practical ways to carry out Threat Modelling *well*. In our opinion, this is the most important aspect to consider when conducting Threat Modelling. Doing Threat Modelling with the right mindset and approach is likely to be the single biggest factor bearing on the effectiveness and usefulness of Threat Modelling. While there are differences between frameworks, and we recommend the use of STRIDE, that choice is significantly less important.

This recommended approach of synthesising OWASP-TMP and STRIDE is outlined below. More details about our consideration process, and the full set of Threat Modelling frameworks and methodologies that we considered are summarised in Appendix B.

4.4 OWASP Threat Modelling Methodology

The Open Web Application Security Project (OWASP) has brought together a range of highly regarded Threat Modelling experts and proposed a set of widely accepted values and principles for best practice guidelines for how to conduct an effective Threat Modelling process (a Methodology). These best practice guidelines are known as the 'Threat Modeling Manifesto'.[173] The Manifesto provides a high-level summary of the preferred approach to be followed when conducting any Threat Modelling, regardless of which particular Threat Modelling framework is used, in order to produce a high quality outcome.

OWASP have developed a corresponding structured Threat Modelling methodology OWASP-TMP (the "OWASP Threat Modeling Process"[174]) which aligns with the Manifesto, and which is widely accepted and is supported by a range of tools.

For the avoidance of confusion we note that OWASP is also known for their 'OWASP Top 10' project.[175] The OWASP Top 10 is an excellent report put together and regularly updated by a range of international security experts which outlines the 10 most serious types of Threats to web applications currently, based on the recent experience of the experts. The report is well regarded in the security community. The Threat types that the report identifies are a useful starting baseline for organisations without a strong maturity in cybersecurity, because they suggest the essential things the organisation should focus on in order to achieve an initial basic level of security.

However, despite both coming from the same organisation, the OWASP Top 10 report is not the same as the OWASP-TMP Threat Modelling methodology that we are recommending here. Given the sensitivity of much CDR data, the CDR ecosystem should have a much higher level of security than the minimum baseline identified in the Top 10 report. Further, the Top 10 is predominantly focussed on securing Web Applications, rather than a complex multiparty ecosystem such as the CDR governed by Data Standards.

OWASP has several other emerging projects that are consistent with, but distinct from the OWASP -TMP. These include an API Security Top 10, as part of the OWASP API Security Project, and the OWASP Ontology-driven Threat Modelling (OdTM) framework. These projects are worth considering to be incorporated as part of Threat Modelling, but, at the time of writing, these are still emerging, and should not be considered complete in of themselves.

As a helpful indication of the nature of the OWASP-TMP methodology, an outline of the structured process it follows is set out below in 4 general stages:

1. System Decomposition: Understand the problem and what kind of solution it requires – its depth and nature. What are we working on? What is the scope of the system and bounds?
2. Threat Identification: Identify the Threats to the system; what can go wrong?
3. Identify Countermeasures: Identify countermeasures that would mitigate the Threats; what are we going to do about it?
4. Reflection: Assess the model for depth and breadth of the process; Did we do a good job, and what could be improved for future iterations?

The overall generic process can be defined as *know the system*, *find the attacks*, *establish countermeasures*, *what next*. As stated earlier, identification of countermeasures is outside the scope of our recommendations on Threat Modelling.

We briefly explain each of the *relevant* stages below (noting the scope of this Report), being the first two.

4.4.1 System Decomposition

System decomposition is the process of creating a detailed view of the system and its boundaries. There are several aspects to this:

a. identifying and categorising the system components;
b. modelling the interactions among system components;
c. identifying boundaries/perimeters;
d. identifying how and what types of data are transmitted and stored;
e. identifying who/what access levels can view or alter this data;
f. outlining roles and responsibilities of the various participants in the system, and
g. determining when does data crosses privilege boundaries.

One categorisation framework on which to decompose a system is included below.

- **External dependencies**. This applies to Threat Models of specific software or companies where software is being developed. This category is defined as anything outside the system that the development team cannot control but that does affect the data security. Examples include the type of server being run and the devices and browsers used by consumers when interacting with CDR participants. While the CDR is not simply a single software system, one might analogously describe external dependencies as being matters beyond the control of the Chair. This includes

4.4 OWASP Threat Modelling Methodology (continued)

higher level elements of the CDR (in the CCA and CDR Rules) as well as the systems used by Data Holders and ADRs as well as partner specific implementations of the API based on the specifications in the Data Standards.

- **Entry points.** These are the ways that an Attacker can interact with the system, categorised hierarchically. There may be several access privileges that exploiting a particular entry point grants an Attacker, depending on the attack. The CDR ecosystem is complex, with many participants and many potential entry points for external and insider Attackers. It is important that the full range of possibilities be identified and considered.
- **Assets.** These include everything of value to the CDR participants and consumers as well as the survival and flourishing of the overall ecosystem. Assets should be organised and exhaustively identified, listed alongside associated trust levels that indicate the level of privilege required to access the asset, the value of the asset to the relevant participants and the cost of losing the asset. Collectively, these factors help assess how important each asset is and identify the owner of the asset and the parties with responsibilities for it or access to it (and in which contexts). Assets range in type from tangible data (e.g. user login details) to intangible assets (e.g. the reputation of the CDR and public confidence in the digital economy). The Chair thus needs to understand how attractive and sensitive CDR data sets are, commissioning additional research if necessary.

  In the context of the CDR, it is important to distinguish assets of the Department of the Treasury (being the relevant Commonwealth entity) and other assets. This is because, while there is responsibility in relation to shared risk, there are different obligations under the PSPF in relation to an entity's own assets. The Treasury's assets include the effective operation of the CDR scheme (as a government program), reputation and consumer confidence associated with its role in issuing Data Standards, and the Data Standards themselves. External assets that may be vulnerable include consumer's privacy interest in the protection of data concerning them as well as the systems and reputations of both CDR Data Holders and ADRs.
- **Trust levels.** These are the participant privileges, and can also be arranged hierarchically as appropriate. The privileges, accesses, and trust relationships of all the participants, systems, and processes in the CDR ecosystem should be fully mapped and clearly set out.

4.4.2 Threat Identification

After system decomposition has occurred, the next stage is to determine what Threats to the system exist. This can be made easier by the use of several frameworks, such as catalogues of existing attacks/attack vectors (e.g. MITRE ATT&CK), Threat categorisation frameworks (e.g. Microsoft STRIDE), or tools, such as attack trees. A Threat categorisation framework such as MITRE ATT&CK, STRIDE, Kill Chain, or Attack Tree can provide a structured process to identify these Threats.

For example, using the STRIDE categorisation approach, the security planners would first examine the system using the lens of spoofing (impersonation) attacks (the S in STRIDE is for 'Spoofing'), checking each component, process, actor, and pathway to notice where and how this class of attack could occur.

Other categorisation frameworks such as Lockheed Martin's IDDIL/ATC framework[176] provide a step-by-step process for identifying potential Threat scenarios through the curated use of known tools, such as Data Flow Diagrams and Threat profiles. Alternatively, several categorisation frameworks can be combined or followed in turn to provide a diverse multi-pronged process. Whichever discovery process is followed, the product of this phase is a comprehensive list of possible attacks on the system. The STRIDE approach is particularly well suited to this phase, as previous applications of the framework have identified which Data Flow Diagram component types are susceptible to which class of attack in STRIDE. The STRIDE Framework is introduced in Section 4.5.

Part of this stage in the OWASP methodology involves determining which attack scenarios / paths are plausible and the vulnerabilities that these attacks exploit. This requires the identification and analysis of the existing protections in the system at all business tiers relevant to the model, including their implementation, weaknesses and efficacy. Viable attack paths can be identified by going through the list of Threats and attacks identified in the previous stage, and applying them to all system components possible. These Threats and attacks are then checked against the existing controls of the system to identify which attack paths are possible and which are blocked or mitigated. Attack paths without controls or protocol protections expose a vulnerability in the system and must be catalogued. This iterative process of selecting a system component, testing it against attack paths, and pruning away the blocked ones can be documented graphically using an attack tree. The information generated by this step helps determine the risk associated with each existing vulnerability, allowing them to be ordered by importance for a later stage in the process (e.g. during a risk assessment).

4.5 STRIDE

We recommend that STRIDE be used in the Threat identification stage of the OWASP methodology as the Threat classification framework for the Data Standards.

STRIDE is a generic and very popular Threat Modelling framework initially developed by Microsoft in 1999.[177] STRIDE identifies Threats using a goal-based approach, whereby security planners consider the goals of an Attacker to identify Threats.[178] The approach is thus based around considering the types of attack which might occur.

The term STRIDE is itself a mnemonic (S+T+R+I+D+E) for six categories of Threat to be considered. These are:

- *Spoofing* – impersonation of authorised users – for example, an Attacker being able to pretend to be a consumer and initiate actions on their behalf
- *Tampering* – malicious altering of information or instructions – for example, being able to alter protocol messages sent to CDR participants to achieve unintended consequences
- *Repudiation* – engineering plausible deniability into an attack – for example, a consumer being able to deny that they have given a consent or a participant being able to deny that they sent a particular message (this has obvious potential for grave consequences if or when Action Initiation is introduced to the CDR)
- *Information Disclosure* – leaking of data outside the system – unauthorised access to the data of consumers, or publication of private data
- *Denial of Service* – halting or impeding of regular system functions – for example, consumers not being able to log into an ADR's the web portal to change their preferences or consents or participants not being able to verify who has been authenticated
- *Elevation of Privilege* – privilege escalation within a system by an Attacker – for example an Attacker being able to impersonate an ADR or Trusted Adviser

The framework serves to categorise potential attacks on a system under these 6 labels. This can be a helpful structure for security planners to prompt them to consider Threats which otherwise might not occur to them.

Due of Microsoft's support, STRIDE has become widely used in practice and is well supported by tools and documentation. It has also evolved and grown in scope over time over time so that it goes beyond Threat identification and includes more functionality. This is both a benefit and a potential challenge as it can be complex to use for those not familiar with it. We feel that the underlying Threat identification framework of STRIDE is very well suited to the Data Standards as:

- The categories into which it organises Threats align well with the likely categories of Threats facing the Data Standards (and also the CDR more generally);
- OWASP itself suggests STRIDE as an effective framework to use in the Threat identification stage of the OWASP methodology;
- It is familiar and well accepted in the security community; and
- It is well supported by tools and documentation.

Hence, we recommend STRIDE be used for the Threat identification stage of the OWASP-TMP Threat Modelling methodology. Note that we do not recommend that the full and far more complex STRIDE methodology be used more widely as the full Threat Modelling Methodology for the Data Standards. For the reasons set out above, the OWASP Methodology will be more effective at supporting and guiding a genuinely collaborative and shared risk approach to modelling the Threats facing the Data Standards and the CDR more generally.

5. Further Considerations

5.1 Maintaining an Effective Threat Modelling Capability

We have been asked to make a set of Recommendations to the Chair as to how to maintain a Threat Modelling capability for Data Standards development.

This section considers issues around establishing and maintaining an effective Threat Modelling capability and ensuring that the Chair is able to be informed to carry out their role. We also consider the issue of dynamic Threats which can be discovered suddenly as a consequence of a successful attack or intrusion underway. Finally, we explore the aspects of Threat related to the customer experience dimension of the Data Standards.

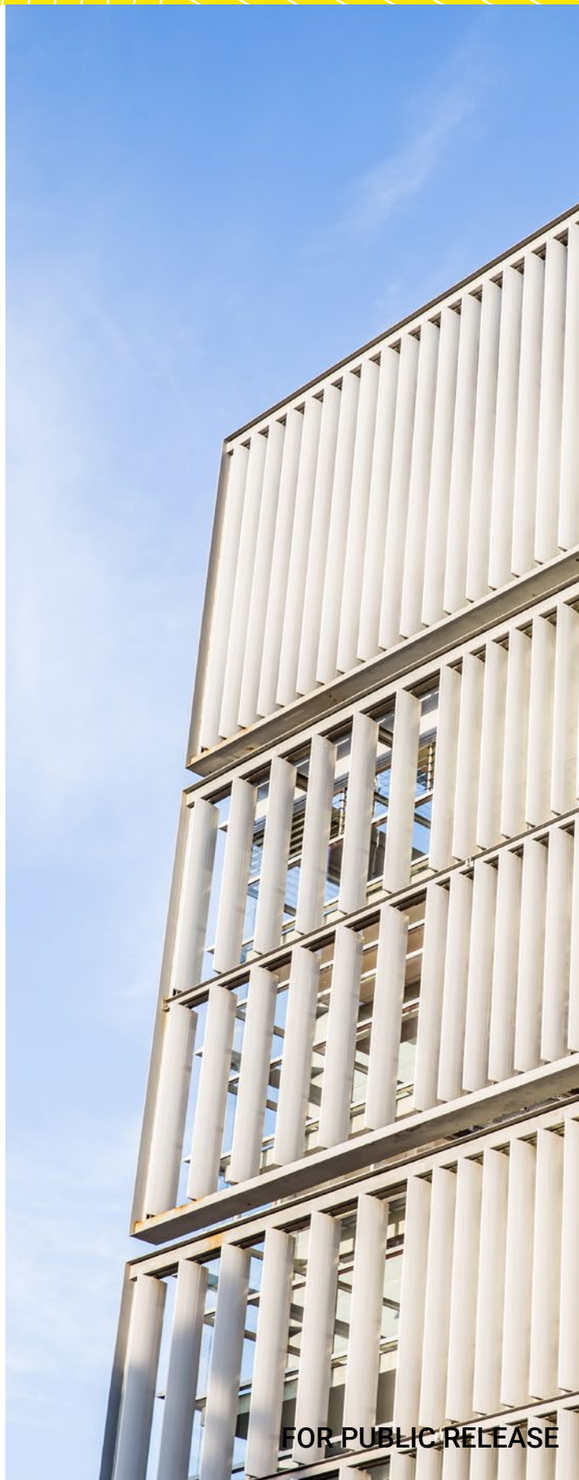
5.1 Maintaining an effective Threat Modelling capability

It is critical that the Chair have access to ongoing Threat Modelling capability to understand current and newly emerging Threats and so conduct appropriate ongoing security planning for Data Standards development. There needs to be sufficient resourcing and internal capacity within the DSB to support the Chair not only in issuing Data Standards, but also in establishing, supporting and responding to Threat Modelling and risk assessments. This includes both financial resourcing for outsourcing self-contained projects to experts where required, and internal human capability to manage and support this process as well to carry out incremental and day to day activities. Human resources need to be sufficient to manage foreseeable emergencies and temporary incapacity, for example due to illness. Staff need the knowledge and skills to cover for each other or where colleagues leave. In particular, they need to understand the system being defended, being the CDR ecosystem. Loss of corporate knowledge about the system can impair the effectiveness of the Threat Modelling process.
The DSB will need to have the capability to deal with any security incidents and emergencies relating to the security of CDR Data and the Data Standards as well as dealing with normal day-to-day operations. Any human capability required to support this may be-in house, or external on-call resources, or a mixture.
Best practice would be to have at least some level of internal capability for coordination and communication rather than the security response capability being entirely outsourced.
Threats arising from resourcing should also be included in the scope of the Threat Modelling activity, since these are critical meta-Threats, that is Threats that can give rise to further Threats. Without sufficient resources to discover and assess Threats, the likelihood and impact of those Threats may increase and new Threats will compound the problems. Loss of key employees without sufficient capability duplication is also likely to reduce the Chair's ability to understand and respond to Threats and otherwise maintain good security governance. There is no point in identifying Threats if there are no resources with which to respond; the scope of Threat Modelling should thus align with the resources necessary for a response. Security is not only about understanding, it is about action.

5.2 Expert Advice to Support the Chair

This section identifies factors that impact how effectively the Chair will be able to benefit from the outputs of Threat Modelling. In other words, it is assumed that an initial formal independent Threat Modelling activity has been conducted in accordance with our recommendations. For the potential benefits of this to be properly realised the Chair must be supported to ensure a sufficiently strong cyber capability and maturity. Once Threats are understood, expert advice can assist the Chair in making decisions about the use of Data Standards to mitigate risks associated with identified Threats. If the Chair is to have sufficient capability to carry out their role through trustworthy Data Standards, enhancing security within the CDR ecosystem throughout the data lifecycle, they will need access to a range of expertise and experience as well as practical assistance.

Best practice would be for the Chair to establish an Expert Advisory Panel to support them in making decisions around security risk, including in relation to their response to the Threats identified through Threat Modelling. The panel would provide expert advice and support in scoping and reviewing the outputs from the initial and subsequent ongoing Threat Modelling, as well as in relation to other cybersecurity activities, such as audits, cyber health checks, and penetration testing. They could also assist in identifying circumstances in which new Threats or contexts require revised modelling.
The panel should be constituted with experts to support the Chair drawn from: representatives from relevant governance bodies (ACCC, OAIC), from academia (cyber technical, risk, incident response, cybersecurity training and communication, psychology, and behaviour), relevant industry expert practitioners, representatives from cyber mature CDR partners, and international representation from one or more overseas open CDR style bodies).



5.3 Data Standards Safety System

Even with a good approach to Threat Modelling and risk management, it is likely that some risk events will occur. While Threat Modelling will inform security planning to help **stop bad things happening**, it is also important to plan for a situation where **they do happen**. The failure to be able to respond effectively to an attack is itself a vulnerability, with its own (often serious) consequences.

The Chair needs to be able to deal rapidly and effectively with attacks or other security related crises when they do happen. For example, if a core-cryptographic protocol used in the secure transmission of data, such as an element of TLS (transport layer security) protocols, is discovered to have a weakness then how should the system respond? How are participants notified? How are corrected standards developed and tested and promulgated under time pressures? What assurance processes are followed? The consequences could be significant and so their scope should be considered and the associated planning carried out *in advance* of such a situation arising. For context it is worth noting that all the cryptographic primitives used in the CDR are eventually expected to break and be compromised. They have been designed with good margins of safety but ultimately they will be broken but the timing of that is unknown.

A **Data Standards Safety System capability should be developed** to allow the Chair to be able to deal rapidly and effectively to security related crises as they happen. This capability will need to include plans, and communication collateral prepared in advance, and be supported by a system to carry out and coordinate technical actions required including forensic logging to help determine post-incident what the root causes were and the extent to which the Data Standards were a contributing factor and need rectification. There will need to be partner training and drill rehearsals at appropriate intervals to test the systems and procedures and human readiness.

The Data Standards provide the common rails for interoperability across the CDR eco-system. The transfer of data between CDR participants, and the management of CDR data across its lifecycle, however, are far more complex than simply agreeing a standardised gauge. Therefore the metaphor for Data Standards security management is more like civil aviation safety, because a data breach is more like an aircraft disaster, than a train derailment. Initially the reporting on the accident will be fragmented and unclear.

Why did it happen? What was the cause? The CDR needs to be able to isolate respective components, much like grounding a particular model of aircraft, until an appropriate solution has been identified, communicated, implemented, and checked. Initially it will be unclear if the Data Standards themselves will be at fault, so there needs to be a clearly communicated plan for how co-ordinated activities will occur during a dynamic, and high-tempo, period. During the early growth-phase of the CDR, ad hoc management of these events may remain possible.

However, especially as the CDR grows, and becomes further entwined into the fabric of the economy, this will no longer be adequate because the number of moving parts will become sufficiently complex, and the continuity of the CDR will likely transition to a point where it becomes essential for the operation of the digital economy; given current policy settings. In this not-to-distant future, the Data Standards Chair will need to be able to rapidly respond to dynamic Threats, with decisive and proportionate action.

Will a pilot need to be grounded because of a near miss? Did the maintenance of a particular plane cause an issue? Or does the whole fleet need to be grounded because of volcanic ash? In the CDR, these examples could be an insecure implementation by a specific CDR participant, a general failure to adhere to the API designs in the Data Standards, and/or the publication of a zero-day vulnerability. How the Chair responds to security issues, such as by providing additional – or revised – guidance, will have an impact of the perception of trust in the CDR.

In all cases there may need to be a response for assurance to be provided to government and industry, but ultimately the public, that their data is in safe hands as it flies across the economy. Consequently, a Data Standards Safety System is required to proactively promote trust and confidence in the CDR.

To address the issues above we recommend that a Data Standards Safety System be developed to facilitate rapid responses to attacks and emergencies affecting CDR data and involving the Data Standards. The system should support the discovery and understanding of any dynamic Threats which arise during or as a consequence of a successful attack or intrusion underway. This should be a system established *before* a crisis and can be based on advice from the Cybersecurity Expert Advisory Panel and in accordance with the ACSC's Cyber Incident Management Arrangements for Australian Governments.[179] The system and associated planning can be shared with other stakeholders, including CDR participants.

5.4 Customer Experience and Understanding as a Contributor to Threat

Amongst the less technical Threats to the CDR ecosystem, there will be a significant category of Threats associated with CDR consumers. Such Threats exploiting human weaknesses and behaviours can be more complex and harder to understand and counter than Threats exploiting purely technical vulnerabilities, for example those relating to data security protocols and cryptographic primitives. Many of these human Threats arise as a consequence of a lack of consumer understanding about the CDR. For example, consumers may authorise a transfer of their data to a Trusted Adviser without realising that this takes it outside the security protocols that apply to transfers between Data Holders and ADRs.

It is in this light that the customer experience (CX) aspect of Data Standards is important. If consumers have an incorrect understanding of the CDR or do not understand what it is that they are consenting to, then they may suffer harm (in particular, through loss of privacy). Misconceptions about the operation of the CDR can be exploited by social engineering attacks (scams and tricks). If consumers believe that their data is protected more than is the case, they can be tricked into believing that those with information about them are trusted parties when, in fact, they are not. By enhancing consumer understanding, CX can diminish the likelihood of successful social engineering attacks. By explaining relevant aspects of the legal framework and CDR ecosystem, consumers come to know what to expect in their interactions with the CDR. Such knowledge facilitates more accurate expectations about their interaction experiences with the CDR, leaving a smaller window of misconceptions for social engineering Attackers to exploit.

Threat Modelling should thus involve expertise in psychology and behaviour and include consideration of CX and Threats associated with a potential lack of consumer understanding of the operation and risks associated with the CDR and their interactions with it.

Glossary

ACCC is the Australian Competition and Consumer Commission

Accountable Authority has the meaning given in the PGPA Act. The Accountable Authority of the Department of the Treasury and the DSB is the Secretary.

Accredited Data Recipient (ADR) has the same meaning as accredited data recipient in CCA s 56AK.

Action Initiation refers to the recommendation that the CDR should enable third parties to initiate actions beyond read-only requests for data sharing.

Advanced Persistent Threat (APT) are Threat Actor groups with sophisticated levels of tradecraft, cyber capabilities and significant resources which allow them to use multiple attack vectors (e.g., cyber, physical, and deception) over an extended period. APTs are often Nation State Actors.

Attacker refers to a Threat Actor with malicious motivations.

Authorised means within the scope of legal requirements and permissions, including statutory requirements and the terms of any policy or notice provided to affected persons and any relevant consumer consent, and not an act or practice that is otherwise misleading or deceptive.

Australian Cyber Security Centre (ACSC) within the Department of Home Affairs leads the Australian Government's efforts to improve cybersecurity.

Availability is the property that data or information is accessible and useable upon demand by an authorised person.

CCA refers to the *Competition and Consumer Act 2010* (Cth).

Chair means the Data Standards Chair.

CSO means a Chief Security Officer (a role within the PSPF).

Confidentiality is the property that data is not made available or disclosed to unauthorised persons or unauthorised processes or for use in an unauthorised manner. Disclosure of data within an entity for use in an unauthorised manner is an adverse event that affects confidentiality of that data, even where there is no disclosure to persons or entities external to that entity.

Consumer Data Right (CDR) is established in CCA Part IVD.

Controls are measures taken to counter Threats.

CDR data has the same meaning as in CCA s 56AI.

CDR ecosystem refers to the network of Data Holders, ADRs, Trusted Advisers, CDR consumers and CDR data.

Competitive Intelligence Threat Actors refers to entities who conduct cyberattacks against rival organisations with the objective of gaining a commercial or competitive advantage over the compromised victim.

CX refers to Customer Experience.

Cybercrime encompasses cyber-dependent crimes (based around information and communications technologies) and cyber-enabled crimes (where information and communications technologies are used to commit offences that could be committed without them). Examples of cyber-dependent crimes include:

- **Computer Access Crimes (CAC)**
  Getting into a computer network or device without permission to obtain information or data. Victims may discover that another person has gained access to their digital device without their permission and has added, removed or made use of information or data, such as credit card numbers, a document, photos or video files or taken personal identity information for illegal purposes. Computer access crimes do not include the acquisition and misuse of credit card information simply through theft, misuse of a card during a normal transaction, nor when a victim is scammed into freely disclosing information

- **Computer Disruption Crimes (CDC)**
  The disruption of computer or network resource operations. Signs that an individual's device has been attacked include the device not working properly or ceasing to work completely, slowed data processing, unusual messages appearing on the device, or the owner being blocked from using the device or being unable to access files because they have been encrypted. These attacks may be accompanied by a ransom message demanding payment to restore the system or decrypt the data.
- **Computer Malfunction Crimes (CMC)**
  When users are uncertain if they have experienced a computer access crime or a computer disruption crime but have experienced a computer malfunction affecting the operation of their devices, networks or information and they believe this was caused by criminally-motivated people.

Cybercrime Groups refer to Attackers who undertake cyber security attacks for the purposes of stealing data, committing financial crimes and extorting victims. They typically include both traditional organised crime groups and Organised Cybercriminals.

The **Dark Web** is an intentionally hidden part of the internet that cannot be accessed using regular web browsers or search engines. Generally it consists of layers of encryption and hidden internet sites which can only be accessed through specialised browsers such as The Onion Router (Tor).

Data Holder has the same meaning as data holder in CCA s 56AJ.

Data Standards refers to data standards issued by the Chair in accordance with the provisions of Division 6 of CCA Part IVD.

Data Standards Body (DSB) is a secondary statutory structure contemplated in Subdivision C of Division 6 of CCA Part IVD. The Department of the Treasury is currently appointed as the DSB.

A Denial of Service (DoS) attack is typically where an attacker does not break into a target machine but rather overwhelms it with a flood of incoming network packets so it ceases to be able to provide its intended services. See also Distributed Denial of Service (DDoS).

Distributed Denial of Service (DDoS) is a subclass of Denial of Service attacks where an attacker causes multiple machines on the internet, typically in the range of thousands to millions of machines, to attack the target. This permits a much greater volume of attack packets to be sent compared to a simple DoS attack from a single machine. The attacking machines do not typically belong to the attacker; usually they are previously compromised machines belonging to a range of non-malicious third parties collectively often known as a botnet.

DTA means the Digital Transformation Agency.

Exploit refers to software, commands or data used to take advantage of a vulnerability in a system to cause behaviour unintended by the original developers.

Hacktivist Threat Actors refer to an individual or groups of individuals who are motivated by ideology and who seek to compromise technology environments to carry out political, social or religious activism.

Information Security Manual (ISM) has the meaning given in PSPF Policy 11. The purpose of the ISM is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber Threats. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cybersecurity professionals and information technology managers.

Integrity is the property that data has not been altered or destroyed in an unauthorised manner.

Likelihood means the probability that a given threat event is capable of exploiting a vulnerability to cause harm.

MaaS refers to Malware as a Service.

OAIC is the Office of the Australian Information Commissioner.

OWASP-TMP is the "OWASP Threat Modeling Process", available online. Note the US spelling of "Modeling" in the title.

Nation State Actors refers to Threat Actors that are part of an entity directly controlled by a sovereign government or who receive direction, technical assistance or funding from a sovereign government.

PGPA refers to the *Public Governance, Performance and Accountability Act 2013* (Cth).

Privacy Safeguards are set out in CCA Pt IVD Div 5.

Pt IVD refers to Part IVD of the CCA.

RaaS refers to Ransomware as a Service.

Risk refers to the effect of uncertainty on objectives.

Risk management refers to the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Risk Management Framework (RMF) has the same meaning as that term in the Risk Policy. It is a structured process for identifying and analysing risks, vulnerabilities to Threats, vulnerabilities, likelihood of Threats, and likelihood and impact of harms. That process is intended to be used to determine whether, when, how, and to what extent particular risks and vulnerabilities should be addressed through actions taken by an entity, and to guide an entity to establish a system of safeguards to mitigate risks and vulnerabilities, and associated controls to assure and verify that these safeguards operate reliably, such that residual risks (after operation of these safeguards and controls) of relevant harms are very low. See further Australian Standard AS ISO 31000:2018 Risk Management Guidelines at Section 5 - Framework.

Risk Policy refers to the Commonwealth Risk Management Policy.

Rules refers to the Consumer Data Rules made pursuant to CCA Part IVD Div 2A.

Secretary means the Secretary of the Department of the Treasury.

Security standards are standards that address how an entity (1) ensures the confidentiality, integrity, and availability of CDR data that it creates, receives, maintains, or transmits; (2) protects against any reasonably anticipated Threats and hazards to the security or integrity CDR data; (3) protects against uses or disclosures of CDR data that are not permitted; and (4) ensures compliance by its personnel, subcontractors and other persons and entities for whom that entity is responsible with the above.

Threat is anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them.[180]

Threat Actor is an entity that is partially or wholly responsible for an incident that impacts or has the potential to impact an organisation's security.

Threat Profile is a tabular representation of all Threats and their corresponding attributes.

Threat Modelling, for the purposes of this Report, focuses on the use of formal frameworks and methodologies that lead to the comprehensive identification of Threats..

Threat sources means the sources of the Threats causing a negative impact on CDR data and stakeholders in CDR data, including CDR consumers. Threat sources may be Threat Actors or events.

Trusted Adviser has the same meaning as in CDR rule 1.10C.

Trusted Insiders refer to an organisation's internal staff and an organisation's trusted key parties whose conduct causes data security incidents. They can be made up of malicious staff, compromises staff, and careless staff.

UNSW Risk Report means Lyria Bennett Moses, Katharine Kemp, Peter Leonard, Rob Nicholls, *Risk Management for the Consumer Data Standards: A report to the Data Standards Chair* (UNSW, 2022).

Vulnerabilities are flaws or weaknesses in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a Threat event.

Watering Hole Attack a type of cyberattack that targets specific groups of users by infecting websites that they commonly visit to deliver malware or misinformation.

Appendices

Appendix A: Attack Types

The cyberattacks that Threat Actors will most regularly deploy against the CDR and CDR participants include:

› **Malware**
Malicious Threat Actor attacks are a certainty for CDR participants, but these attacks come in many forms. Malware is one form, which is a software used by to access an organisations' internal networks.[181] Almost half of small to medium enterprises in Australia have experienced this form of attack.[182] Therefore, CDR participants, including small to medium FinTechs, will likely be attacked by malware. The most common Australian industries impacted by malware were accommodation and food services, construction, wholesale trades, manufacturing and transport, postal and warehousing. A number of these industries will partially align with the sectors that are currently part of the CDR or may become part of the CDR in future.

Malware as a Service (MaaS) remains prominent within the criminal enterprise markets, used by criminals who lack the expertise or knowledge to deploy their own cyberattacks. MaaS is used to steal sensitive and personal individual datasets.[183]

Another form of malware is destructive malware, which makes targeted systems or files completely unusable, causing significant recovery costs for organisations, as seen in the Sony Pictures Entertainment cyberattack.[184] Threat Actors are continually looking to advance their tactics and techniques and evidence suggests that popular malware forms are being replaced with new compromise methods.[185] As data exchanges are being performed in line with the requirements set out by the DSB, data could be intercepted by Threat Actors if an API endpoint is infected with Malware.

› **Denial of Service and Distributed Denial of Service (DDoS)**
Denial of Service attacks are cyberattacks that overwhelm a system, typically with large volumes of fake network traffic, potentially causing business interruption and financial loss.[186] Distributed Denial of Service (**DDoS**) is a subclass of Denial of Service attacks where an attacker causes multiple machines on the internet, typically in the range of thousands to millions of machines, to attack the target system. This permits a much greater volume of attack packets to be sent compared to a simple DoS attack from a single machine. The attacking machines do not typically belong to the attacker; usually they are previously compromised machines belonging to a range of non-malicious third parties collectively often known as a botnet. These attacks can also be deployed as part of a larger multi-stage attack, for example to disable a critical system and so assist the Attacker to launch a ransomware or another cyberattack in order to encrypt or extract crucial datasets.[187] In 2018, GitHub experienced such an attack, however given the strong protections that had been implemented, GitHub's systems were only inoperable for a short period of time.[188] Data Holders, ADRs and Trusted Advisers will experience DDoS attacks where Threat Actors target system operations and availability. A successful DoS attack could make a CDR participant's services unavailable, threatening the reputation of the CDR and consumer trust in the overall security posture.

› **Ransomware**
ACSC reported a 15% increase in ransomware incidents during 2020-21.[189] Ransomware attacks involve the use of specialised malware deployed on an organisation's system that both encrypts and extracts data.[190] Attackers often demand a cryptocurrency payment in return for the data or deletion of the data.[191] The prevalence of ransomware attacks in Australia is rising, and nearly 80% of ransomware attacks in Australia during the first half of 2021 involved the Threat of leaking exfiltrated data,[192] which increases the leverage an Attacker has by not only limiting the availability of critical information but also threatening to disclose sensitive data.

The Incident Scenario in Section 2.3.2, demonstrates that, as Data Holders and ADRs transfer and use CDR data, they will be attractive targets. This is due to both the intrinsic value of CDR data and the business impacts ADRs and Data Holders will sustain where they suffer a data availability or data integrity incident.

Ransomware attacks create significant financial exposures for these organisations. Double and triple extortion methods will also be a concern. The CDR will be susceptible to all these extortion methods. These methods are seen where multiple extortions follow successful ransomware attacks, which prey upon reputational harms such as publication of exfiltrated data and frauds carried out directly against clients of impacted organisations. As seen in the Incident Scenario, a ransomware attack may also threaten wider community confidence in the CDR regime, and could impinge upon the successful ongoing rollout of the CDR.

› **Ransomware-as-a-Service**
The majority of Threat Actors are motivated by financial gain and are driven by strategies that will facilitate large financial extortions from victims. They use techniques that require the least possible effort and that are repeatable. These factors have resulted in the increased adoption of Ransomware as a Service (**RaaS**) models. RaaS allows sophisticated Threat Actors to reduce their risk within the criminal ecosystem and allows less mature Threat Actors to obtain toolkits and support services.[193] Organised RaaS groups regularly sell or rent hacking tools to Threat Actors or Threat Actor Groups, who then use these tools to perform extortion attacks against victims.[194] Threat Actors pay for RaaS services through monthly subscription flat fees, affiliate programs which include profit sharing going to the RaaS developer, licensing fee models, and profit sharing arrangements.[195] By leveraging RaaS services, Threat Actors are able to significantly scale up the reach and extent of their operations. RaaS also allows Threat Actors with limited technical knowledge to launch ransomware and extortion attacks against a wide variety of organisations and individuals involved in the CDR. Threat Actors with RaaS capabilities will have the means to disable and cause disruption to Data Holders', Trusted Advisers' and ADRs' critical business systems and impact their ability to provide services.[196]

RaaS commonly facilitate data exfiltration and extortion tactics, allowing Threat Actors to threaten to leak an impacted organisation's data if ransoms demands are not met.[197] Compromised ADRs will be unable to process client requests or conduct key business activities. Compromised consumers face unintended disclosure of sensitive CDR data. Compromised Data Holders face significant CDR data exfiltration and cyber extortion exposure and where these organisations are compromised they will be unable to process client requests or conduct key business activities.

The Organised Cybercriminal group 'Wizard Spider', discussed in Section 2.3.2 (Incident Scenario) produces RaaS software and is reportedly responsible for the creation of numerous ransomware and trojan software tools used in cyberattacks globally.[198] For example, Ireland Health Service Executive[199] and US law enforcement and medical service agencies[200] experienced cyberattacks from Wizard Spider's RaaS models. The organisations experienced extortion demands, and significant business interruption and the Ireland Health Service attack led to widespread impact, resulting in multiple hospitals being inoperable, appointments cancelled, and sensitive patient and employee data stolen. Data Holders and ADRs will face consumer and public reputation damage and potential regulatory penalties if personal data is lost or leaked.

The range of attacks that Threat Actors will perform include:

› **Data Scraping**
Data scraping is an attack method used by malicious actors. It is the act of web or server data 'scraping'. Scraping is a technique for extracting data where the Attacker requests consolidated information from a server using commands similar to those that a legitimate program might employ in the ordinary course. There is significant concern within the cyber security industry that malicious Actors will increasingly attempt API scraping attacks which can result from (amongst other things) security misconfigurations, assets management weaknesses, and the crafting of unexpected API requests.[201] This evolving area of cyber security is foreshadowed to become a focus of Organised Cybercriminals.

› **Software Vulnerability Exploitation**
Software vulnerability exploitation is an attack that takes advantage of vulnerabilities in applications, networks, operating systems, or hardware, usually taking the form of software or code that aims to take control of computers or steal network data. Many other forms of malicious compromises are facilitated by vulnerability exploitation, which often provide either the initial means of ingress into an organisation's environment, or the means to traverse the organisation's internal environment.

In March 2017, Equifax experienced a cyberattack that exposed 145 million peoples' personal information and 200,000 credit card numbers. Unauthorised access occurred though a known vulnerability that Equifax failed to sufficiently patch due to poor internal system monitoring, permitting Threat Actors to exploit systems and allowing direct access to Equifax sites and data bases.[202] A patch had been released, however reportedly an employee did not deploy the patch and scans did not pick up on the undeployed patch.[203] This illustrated how one key vulnerability can lead to wide ranging consequences enabling the Threat Actor to gain access and exfiltrate data.

Threat Actors monitor the release of critical vulnerability patches and will launch cyberattacks accordingly. Vulnerability exploitation was a top concern for Australia, with Threat Actors attacking organisations the same day announcements of vulnerabilities occur, leaving little time for the implementation of the released patches.[204] Where parties to the CDR do not

Appendices

have sufficient security and preventative measures Threat Actors will exploit vulnerabilities, and this could foreseeably expose consumer personal and financial data across the entire CDR regime.

› **Supply chain cyberattack**
Supply chain cyberattacks target retailers, manufacturers and distributors who provide products or services to other organisations.[205] Threat Actors leverage the connection between an organisation and their supply chains to target more than one entity from a single cyberattack. Compromised ADRs and Data Holders will threaten the greater CDR regime where cyberattacks transcend an initial attack point and impact third party organisations or CDR participants. The connectivity of CDR participants threatens the wider ecosystem if supply chains are attacked, and Threat Actors circumvent the security measures of data sharing platforms. Over the past 12 months, the most common types of supply chain attacks recorded in the claims data of the global cyber insurer Allianz were targeted compromises against technology service providers who have elevated privileges within their client's IT environment and attacks which target physical supply. Numerous noteworthy cyber breaches in Australia have been caused by supply chain compromises.[206]

The CDR is an attractive supply chain target for Threat Actors. Due to the interconnected nature of the CDR, compromises of a CDR participant may provide ingress points to attack other Data Holders, ADRs or other third parties. Threat Actors will likely examine potential weaknesses within the Data Standards, given these are open source. As the CDR expands and ADRs and Data Holders can on-share consumer data with further third-party entities, there will be heightened Threats of supply chain cyberattacks and widespread impacts on entities who have interactions with these parties. Any cyberattack leveraging the Data Standards would provide grounds for supply chain attacks against the wider CDR community.

› **Social Engineering**
Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Some examples of social engineering are email and SMS phishing, phone scams and luring users to malicious websites. Threat Actors also facilitate strategic boiler room schemes. A boiler room is an outgoing call centre that offers recipients services or products, insinuating that they can provide them with significant investment opportunities or some type of financial benefit.[207] It is foreseeable that Threat Actors will falsely portray themselves as ADRs or Data Holders, offering CDR consumers false services or price competitions, leading those consumers to provide personal or financial information to these individuals.

› **Password Attacks**
Password attacks encompass a variety of methods used by a Threat Actor to guess or steal passwords. Common examples include brute forcing passwords (i.e. randomly guessing passwords for a single resource by cycling through all available password combinations) and credential stuffing (trying a known username and password combination on a variety of other websites and services used by an individual). A password attack on an ADR or Data Holder will provide an Attacker with access to internal networks and the ability to directly compromise CDR data and wider IT environments.

› **Business Email Compromise**
Business email compromise is used to obtain access to email accounts and mailbox data of an individual. Once compromised, these emails can provide a staging point to attack other parts of an organisations technology assets or be leveraged to attempt financial frauds such as funds transfers and redirection frauds. Common redirection frauds include amending payment details where an Attacker has intercepted and altered emails that appear to come from a legitimate third party. These frauds regularly succeed because employees do not seek further clarification given the communication appears to originate from a known source.[208] More than 3,300 BEC incidents were reported in 2021,[209] with an average loss of $50,600 each successful intrusion.[210] Unauthorised access to ADRs' and Data Holders' mailbox data will expose CDR data and allow access to other critical business systems. In 2022, Nigerian police arrested members of 'SilverTerrier' a well-known organised criminal syndicate that facilities business email compromise scams.[211]

› **Watering holes**
Watering holes is a technique Attackers use to infect legitimate websites that a victim visits regularly for the purpose of compromising the user.[212]

› **Spear-phishing**
The targeting of specific (as opposed to all) individuals with fraudulent emails, texts and/or phone calls to steal login credentials or other personal information.

› **Zero-day exploits**
The use of unknown security vulnerabilities or flaws in software prior to the discovery and patching by the developer or IT team.[213]

Appendix B: Review of formal Threat Modelling approaches

For comprehensiveness, in this section we briefly outline the commonly used Threat Modelling approaches which are used by security planners. We give a brief commentary for each analysing the relevance of the approach to Threat Modelling for the Data Standards, and for the CDR more broadly. The Threat Models described are:

1. STRIDE
2. Mitre ATT&CK
3. OCTAVE
4. OWASP-TMP
5. LINDDUN
6. DREAD
7. NIST Special Publication 800-154, Guide to Data Centric Threat Modelling
8. Intel's Threat Agent Risk Assessment (TARA) and Threat Agent Library (TAL)
9. IDDIL/ATC
10. Attack Lifecycle or Cyber Kill Chain

1. STRIDE
STRIDE is a generic and widely used approach to Threat Modelling initially developed by Microsoft in 1999, and expanded considerably since.[214] STRIDE Threat Modelling follows a goal-based approach where security planners consider the goals of an Attacker, based on a framework based on common attack categories. Following the STRIDE framework helps planners to discover and identify Threats in a holistic way.[215] The term STRIDE is itself a mnemonic for six types of attack considered in the framework: *Spoofing* (impersonation of authorised users), *Tampering* (malicious altering of information), *Repudiation* (engineering of plausible deniability into an attack), *Information Disclosure* (leaking of data to outside the system), *Denial of Service* (halting or impeding of regular system functions), and *Elevation of Privilege* (privilege escalation within a system by an Attacker). The following table sets out a high-level view of the STRIDE Threat categorisation framework and the types of security controls that are effective to mitigate each category.

	Threat	Australian Privacy Principles	Countering Control
S	Spoofing	Impersonation by stealing identity credentials	Authentication
T	Tampering	Unauthorised alteration or change of data	Integrity (Hashing)
R	Repudiation	Deniability of wrong events	Non-repudiation
I	Information Disclosure	Exposure of data to unauthorised person or system / data leakage	Confidentiality, Privacy
D	Denial of Service	Service Unavailability	Availability
E	Elevation of Privi-leges	Increasing rights to access assets	Access Control

Appendices

STRIDE is ubiquitous, used in a wide variety of domains due to its generic categorisation of Threats. Consequently, several case studies assessing the frameworks applicability and utility in differing contexts exist in the literature, including in industrial control and cyber-physical systems, web applications, and peer-to-peer architectures. Methods for applying STRIDE have also been well documented and these can be used as a baseline to apply the framework relatively quickly. STRIDE's long-lived presence in the security community and the support provided by Microsoft has also meant that several resources are available that combine the framework with other tools (such as Data Flow Diagrams) to make the Threat Modelling process more efficient. However, because the framework is so general, it may not accurately reflect or organise the most prevalent attacks in a particular domain as well as frameworks designed for them. The framework may be adapted to a specific domain, but this can be time-consuming, and the resulting framework may end up hindering the Threat Modelling process. STRIDE is one of the oldest frameworks for Threat Modelling still in active use.

The process for STRIDE is as follows:

- Define what is being developed. Anecdotally, this process considers the development of components and interfaces, with a focus on trust boundaries.
- Consider potential adversaries and their objectives.
- Apply the attack vector categories of the STRIDE mnemonic to all components and interfaces.
- Identify potential flaws and security issues based on the outcomes of the previous stage. Listed attack vector mitigations can be discussed and implemented.

Criticism and Limitations
STRIDE was developed specifically to integrate into Microsoft software development processes, and this creates implicit requirements and limitations in how it operates in other contexts. The relatively simple nature of the process is less of a structured methodology and more of a considered list of Threat types. This lack of structure has both advantages and disadvantages – it is less prescriptive and can be applied to a wide variety of contexts. This high-level perspective has ensured that it is still relevant. The chief disadvantages of STRIDE are its age, and the consequent challenges in updating a methodology to align with changes in security best practice and a more evolved understanding of the security planning community over time. The challenge is simultaneously having to cater to a wide base of existing users and practitioners who are familiar with the established approaches and software tools developed for them. Its general nature means there is a trade off with the detail it provides and that it does not directly address specific attacks. The categories it uses are broad and require additional expert interpretation to be effective.

Applicability to the Data Standards
Numerous attempts have been made to apply STRIDE to financial sectors with some success.[216] This shows that the framework has promise for CDR Threat Modelling, however certain categories (in particular Tampering) may have to be further sub-divided to avoid too many Threats coming under the same generic prompt, and so the prompt risks losing some of its effectiveness in helping security planners identify Threats. If used in practice in the Data Standards Threat Modelling, as this Report recommends, the planners should consider a further sub-categorisation based on, for example, Attacker objective and/or capability. If the right categorisation system can be devised based on STRIDE, it can illuminate the underlying system vulnerability that Threats exploit (for example spoofing might point to faulty authentication procedure or careless handling of login data). It should be noted that in recorded applications of STRIDE, attacks often blurred boundaries, appearing under several categories.

More specifically, STRIDE will require the use of domain experts to translate the high-level Threat categories into more precise Threats that are applicable to the CDR and Data Standards. The high-level nature of STRIDE ensures its adaptability. STRIDE is widely used in Australia, particularly in government. Therefore, its adaptation in the government and financial sector will be easier. Microsoft has developed and maintained a free tool to assist with Threat Modelling using STRIDE.[217] Hence, the use of STRIDE to model Threats in CDR with the banking sector as an example would be easier.

2. MITRE (ATT&CK) Framework - Adversarial Tactics, Techniques & Common Knowledge
In 2013, in order to better understand cyber Threats, the MITRE corporation developed the Adversarial Tactics Techniques & Common Knowledge (ATT&CK) Framework.[218] The ATT&CK framework has a large database that is a catalogue of known attack paths used by Attackers to harm organisations, mobile devices, financial systems, and industrial control systems, categorised by

Attacker objectives.[219] The database includes descriptions of each attack, real-world instances where the attack was executed, mitigation strategies, and where available, by whom these attacks are perpetrated. It includes attacks on a wide variety of enterprise system types, including servers and corporate endpoints (Windows, MacOS, Linux, cloud platforms, etc.), mobile devices, and ICS (including HMI and SCADA systems). Some examples of Attacker objectives include **persistence**, **evasion**, and **privilege escalation**, and some attacks listed under them include project **file infection**, **masquerading**, and **hooking through APIs**.

ATT&CK is widely used within the community, but not as a Threat Modelling framework, rather as a tool that can be applied in many use-cases, including within existing Threat Modelling frameworks.

In the ATT&CK framework, tactics represent the low-level goals an Attacker has whilst performing a cyber operation. The ATT&CK framework seeks to describe all possible types of action an Attacker might carry out, at a tactical level. The ATT&CK framework includes functions that may, under normal circumstances be benign in nature, but may also be used by an Attacker. Such processes are difficult to detect without creating false-positive alerts. The qualitative nature of ATT&CK framework also seeks to connect intelligence between the tactical, operational and strategic levels. This approach has several benefits, allowing executive leadership to consume strategic intelligence to prioritise resources, at an operational level, providing assistance for Threat analysis and vulnerability management, and at a tactical level, providing insight into security tools and processes.

Criticism and Limitations
The ATT&CK framework can be of great value to security planners and defenders. However, it is not a self-contained Threat Modelling methodology in of itself, or a complete Threat categorisation framework. Rather it is a (large and useful) collection of known examples. It has the benefit of containing known attacks on financial systems, organised by Attacker goals relevant in the domain.

ATT&CK can be used to bolster a chosen Threat Modelling framework, such as STRIDE, by providing a rich set of specific attack scenarios to consider. The wide variety of attacks described provide valuable prompts during the Threat identification phase of the Threat Modelling process, as the system can be tested against each one to see which it is susceptible to. However, the database is not perfect. Several attacks are described in generic terms that could be applied to almost any system, such as 'exploiting software vulnerabilities', applicable to all software. Attacks are also not strictly bound to their category within the database, and several can be used to achieve multiple Attacker objectives, which somewhat lessens the utility.

Applicability to the CDR
The main utility of the ATT&CK framework from the perspective of CDR are the attacks specific to the financial system, useful to augment Threat discovery in the ways described above. Some attack categories (persistent, privilege escalation) map well onto STRIDE, however others (like evasion), do not. Regardless, the method of categorising attacks may serve to modify existing Threat Models for improved applicability to the CDR system. Above all else, the attacks themselves provide an accurate relevant resource for exposing Threats.

In summary although ATT&CK is not suitable as a Threat Modelling framework in the traditional sense it is still valuable as a source of Threats examples, and can be used to augment existing frameworks, such as the OWASP-TMP + STRIDE approach recommended in this Report.

3. OCTAVE
OCTAVE is the **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation framework, developed and subsequently maintained by Carnegie Mellon University in 2001. OCTAVE was developed primarily for large organisations that seek to identify and reduce their information security risks. Variations on the methodology exist for larger (300 or more employees) and smaller (100 or fewer employees) organisations.[220]

The OCTAVE methodology follows a process broken down into asset identification, information infrastructure vulnerability detection, and finally development of a risk mitigation strategy.[221] This process is standard across many Threat Modelling frameworks, but OCTAVE's main focus is on the first and last steps of this process. A greater emphasis is placed on modelling information systems and mapping them to company assets than the identification of Threats to the system. This framework approaches risk mitigation largely from the defender's perspective, focussing on assets to be protected more than on specific attacks.

Appendices

Criticism and Limitations
The procedure to conduct OCTAVE Threat Modelling is well documented, with several new variations on the standard model released (OCTAVE-FORTE being the most recent iteration).[222] This quality ensures a high degree of reproducibility when conducting Threat Modelling, a useful feature when assessing an organisation's risk posture over the long term. However, it can be argued that, compared to STRIDE, OCTAVE's lack of focus on vulnerability identification would be more likely to lead to Threats being missed and so to blind-spots, or a failure to recognise vulnerabilities in the system that a common attack pattern could easily exploit (for example a replay attack when authenticating users might be difficult to see from behind an organisation's login portal).

Applicability to the CDR
OCTAVE is well-regarded within the security community generally. However, its adoption in the financial sector is limited. The high-level nature of OCTAVE means it is less prescriptive, which is positive for CDR. However, it would likely require additional expertise to translate the high-level Threats identified into actionable Threat detail. As a methodology, OCTAVE is comprehensive in the helpful Threat Modelling guidelines to provides, but it will be complex to use. Finally, there is no tool available to structure Threat Modelling with OCTAVE. Therefore, its use in CDR would be challenging.

4. OWASP-TMP Threat Modelling methodology
The "OWASP Threat Modeling Project" (https://owasp.org/www-project-threat-model/) is a project aimed at creating an information source on Threat Modelling techniques, in a framework-agnostic manner. It is based around a 4-question structure to help organise Threat Modelling:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?

Below is an explanatory extract from the methodology:[223]

> *The basic Threat Modelling process consists of the following steps. The process of exploring the search space can be iterative and refined. It is common to mistakenly think you should filter for "the most important threats" early, but how can you do that before you've found them?*
>
> 1. ***Assessment Scope** – The first step is to ask what are we working on? This might be as small as a sprint, or as large as a whole system.*
> 2. ***Identify what can go wrong** – This can be as simple as a brainstorm, or as structured as using STRIDE, Kill Chains, or Attack Trees.*
> 3. ***Identify countermeasures or manage risk** – Decide what you're going to do about each threat. That might be to implement a mitigation, or to apply the accept/transfer/eliminate approaches of risk management.*
> 4. ***Assess your work** – Did you do a good enough job for the system at hand?*

There are numerous helpful resources available such as the OWASP Threat Model Cheat Sheet, which is a document designed to both guide security planners through the entire process of Threat Modelling, and to also provide a single point of reference for users who just need some simple information on a specific area of Threat Modelling. It breaks the process down into the following areas:

- Pre-work/Getting Started
- Decompose and Model the System
- Identify Threat Agents
- Write your Threat Traceability Matrix
- Determine Countermeasures and Mitigations

Pre-work/Getting Started:
Before you can get started on creating a Threat Model, OWASP-TMP recommends a number of actions and decisions that should be taken beforehand to prepare yourself. They suggest that you take time to define your business objectives, create a flow diagram of

the system you intend to perform the modelling on in order to develop a thorough understanding of it, and create design documents for the system (if they do not already exist). This work, while extensive in some cases, will help ensure that your Threat Model is comprehensive and founded on a strong understanding of the system.

Decompose and Model the System:
To begin building your Threat Model, you need to gain a strong understanding of the system. OWASP recommends starting this process by creating a high-level information flow diagram; which should include trust boundaries, internal and external Actors, information flows, information classification and elements, and assets. To build this system model, and ensure its accuracy and completeness, OWASP recommends the following considerations and suggestions:

- Evaluate assets according to their Confidentiality, Integrity, and Availability (CIA) needs
- Consider whether data is in transit or at rest at any given part of the model, in order to design security as appropriate for these situations
- Whiteboard your architecture, including major constraints and design decisions.
- Present your data-flow diagram in the context of Model, View, Controller design
- Use tools to draw your diagram; existing tools include OWASP Threat Dragon, Poirot, MS TMT, and SeaSponge.
- Define data flows using an organisation data flow diagram (if available).
- Define internal and external trust boundaries.
- Define user roles and trust levels, including level of authorisation in each part of the model.
- Identify your entry points into the application.

Identify Threat Agents:
Once you have finished modelling the system, OWASP suggests you attempt to identify the Threat agents. The 5-step process to conduct this is as follows:

1. Define all possible Threats – Using means, motive, and opportunities, attempt to identify all possible Threats to the system. The OWASP-TMP method recommends that you try to minimise the number of Threat agents by defining them in classes, rather than individuals.
2. Map Threat agents to application entry points – identify where each Threat agent could gain access to the system, such as logins, registrations, and insider access.
3. Draw attack vectors and trees.
4. Map abuse cases to use cases – A list of all possible abuse cases should be developed for each of the applications use cases. This is intended to help identify logical Threats to the applications processes.
5. Re-define attack vectors – Consider the possibility of new attack vectors emerging from your abuse cases. For example, does a compromised user account result in a new attack vector into your system?

Write your Threat Traceability Matrix:
OWASP-TMP partitions this step into 2 parts:

1. Defining the impact and probability of Threats.
2. Ranking your risks.

OWASP suggests you utilise risk management methodology to define the impact and probability of your Threats. The cheat sheet provides 2 example methodologies (DREAD, and PASTA) but there is no requirement to use any particular method. As part of your risk assessment and management, create a risk log for every Threat or attack previously identified. After the risk assessment has completed, risks should be ranked from most to least severe. OWASP recommends using a risk matrix for this and provides a basic example in their cheat sheet, but any method of quantifying and comparing risks is also considered acceptable.

Appendices

Determine Countermeasures and Mitigations:
Identify who will own each risk and decide with them, and stakeholders, what risk mitigation approach is acceptable for their respective risks. As part of your risk treatment strategy, OWASP recommends you follow the Reduce, Transfer, Avoid, and Accept process – where you attempt each step to mitigate the risk, before moving on to the next step with any residual risk. After this process, the risk owner should determine what the appropriate controls are to mitigate the risk, and then test these controls to verify your risk reduction process. OWASP also recommends periodically retesting your risks and re-evaluating your Threats.

OWASP Tools:
The tools that OWASP-TMP provide include:

- Threat Model Cookbook: A collection of actual Threat Models that people have designed and applied for various scenarios. Useful for exposure to how this is done and to what depth.[224]
- Threat Dragon: A diagram creation tool tailored to Threat Modelling.[225]
- OWASP Threat Model Cheat Sheet: A comprehensive cheat sheet of terminology, techniques, and key concepts.[226]
- OWASP Ontology-driven Threat Modeling (OdTM) framework[227]: OdTM is a community-driven approach to Threat Modelling involving the heavy use of structured knowledge and automated reasoning. By default, the OdTM implements the Academic Cloud Computing Threat Patterns (ACCTP) model, but also integrates with the ATT&CK framework. This approach is not designed to compete with other OWASP initiatives, but to complement them by providing a less abstract approach that can work in conjunction with Threat assessment processes. Given the 'incubator' stage of this project, whilst the OdTM forms a valuable resource, it is not one that can be solely relied upon. The future of this work will depend on community engagement.

Applicability to the CDR
As discussed in the body of the Report we recommend that OWASP-TMP (in conjunction with STRIDE) be used to conduct the data standards Threat Modelling, as well as CDR Threat Modelling more generally, for the reasons set out in Section 4.

The OWASP-TMP has a web focus, which is well aligned to the nature of the Data Standards and it will likely elucidate risks specific to APIs. This contrasts with Threat Modelling frameworks that were originally designed for traditional computing infrastructures. There is significant information about OWASP Threat Modelling, and many online resources, which should support ease of implementation. In addition, there is a strong OWASP Threat Modelling community, both in Australia and globally. OWASP is referenced in government cybersecurity publications, including the ISM. The open nature of the OWASP-TMP methodology framework will allow analysts to incorporate other specialised Threat Modelling frameworks. As outlined in Section 4, we recommend that STRIDE be used for this purpose. Historically OWASP Threat approaches have been less used in the Australian government than older methodologies such as STRIDE and OCTAVE, but it is encouraged in this context in the ISM.

5. LINDDUN
LINDDUN is a Threat Modelling methodology that identifies privacy Threats in a software architecture and provides a structured process for Threat Modelling.[228] LINDDUN also offers privacy knowledge to non-privacy experts to argue about privacy Threats, as its analysis is based on system decomposition study. LINDDUN is an acronym where each letter in the name refers to a potential privacy Threat to the components of the system or application:

- **L**inkability: refers to linking two items of interest to same user with high probability (e.g., like request or written query);
- **I**dentifiability: refers to identify user from implicit information i.e., even when the data is anonymized;
- **N**on-repudiation: refers to gather evidence so that a party cannot deny having performed an action;
- **D**etectability: refers to detecting if users data or item exists in a system or a database;
- **D**isclosure of information: is the exposure of information to individuals who are not supposed to have access to it;
- **U**nawareness: refers to leaking to disclosing user information without their knowledge or consent; and
- **N**on-compliance: happens when the system is not compliant with the (data protection) legislation, its advertised policies and the existing user consents.

The LINDDUN process consists of six steps. The first three steps are considered core of the LINDDUN methodology and help in identifying privacy Threats in a software system. The last three steps are more solution-oriented and help in translating the elicited Threats into privacy mitigation strategies and solutions.

In the first step, a model of the system is created using a Data Flow Diagram. The software system is decomposed into logical or structural components and for each of the parts privacy Threats are analysed.

This step is repeated to get a refined model. In the second step, Data Flow Diagram is mapped into Threat categories using a generic mapping table. These categories are basically the acronyms discussed above.

The third step is to elicit privacy Threats through Threat trees that describe the most common attack paths. Each leaf in a Threat tree corresponds to the Threat in a system and is properly documented. The results of the elicitation process is a collection of Threat scenarios which are then documented.

The fourth step is to manage Threats by prioritising them based on their risk i.e., due to time and budget constraints, selecting Threats that are most important ones.

The fifth step is to elicit mitigation strategies to resolve privacy Threats. LINDDUN provides a mitigation strategies taxonomy that maps to each Threat in a Threat tree.

The final step in LINDDUN is to translate the selected mitigation strategies to appropriate privacy enhancing solutions.

LINDDUN is not suitable for use in Threat Modelling for the CDR because it mainly focuses on privacy Threats and does not general Threats to security. It has limited community support, and has not previously been recognised across the whole of government.

6. DREAD
The DREAD Threat Modelling framework was also created at Microsoft, like STRIDE, and is designed for integration into their software development and assurance processes.[229] DREAD stands for Damage, Reliability/Reproducibility (attack reliability / attack reproducibility), Affected Users, and Discoverability. DREAD is designed to work in conjunction with STRIDE, specifically to evaluate and prioritise the defined Threat Actors. For each of these, Threat Actors are qualitatively scaled (1-10) and compared. Microsoft ceased using DREAD in 2010, as it was considered overly subjective and was not effectively reproducible. Whilst there are small communities who still apply modified implementations, it has largely been replaced by other frameworks.

It should not be a consideration for use in the context of the CDR as it is not heavily used except in niche areas and has been overtaken by more comprehensive processes.

7. NIST Special Publication 800-154, "Guide to Data Centric Threat Modeling"
The National Institute of Standards and Technology (**NIST**) has drafted a guide (800-154) that serves as an introduction to data-centric system Threat Modelling.[230] The guide does not define a Threat Modelling methodology, rather the purpose is to educate organisations on the fundamentals of data centric Threat Modelling and to make recommendations on data centric protection. The guide discusses a qualitative approach to Threat Modelling using four stages.

The first stage is to identify and characterise the system and data on interest. This stage narrows down the scope to specific data on a specific host or a small group of closely related hosts and devices. The system and data are then characterised under the system's operations. The characterisation involves authorised locations for the data within the system (i.e., storage, transmission, execution environment, input, and output), understanding how the data moves within the system between authorised location, security objectives for the data, and propel are processed who are authorised to access the data.

The second stage identifies the potential attack vectors of an Attacker based on risk assessments (likelihood and impact). Due to time and budget constraints, organisations can prioritise a subset of attack vectors based on their impact and likelihood.

The third stage addresses the security controls for mitigating specific attack actions and patterns. Feasible risk mitigation controls

Appendices

are identified and documented that helps in mitigating the risks associated with attack vectors.

In the final stage, the Threat Model is analysed to determine all the attack vectors and controls across all the unacceptable risks.

This methodology is a relatively novel approach and has been included in this review to provide visibility and coverage of the possibility of taking a data-centric approach.

We do not recommend using the NIST 800-154 guide to Threat Modelling because it does not have a strong community in Australia, has been in draft since 2016, is very generic and relies on data-centric system owners to identify Threats, and does not provide a framework of Threat categories or a Threat list.

8. Intel's Threat Agent Risk Assessment (TARA) and Threat Agent Library (TAL)

Intel developed Threat Agent Risk Assessment (TARA) in 2009 to identify the potential information security attacks that are most likely to occur. As a first step, the methodology identifies the Threat agents that could harm the system with higher likelihood and the method that they are most likely to employ. Next, the vulnerabilities that could be exploited by that method are identified, followed by steps to minimise the likelihood of occurrence.

Intel has also published a library of Threat agents – the Threat Agent Library or TAL. TAL is designed as an initial reference for the TARA process. TAL defines 22 archetypes, each comprised of 8 attributes: intent, access, outcome, limits, resources, skill, objective, and visibility.[231]

We do not recommend using TARA or TAL to undertake Threat Modelling in the CDR. It is designed to augment a formal Threat Modelling methodology, and is not one itself. Further its intent is only to provide a subset of Threats, pragmatically, and so does not align well with the approach of the PSPF.

9. IDDIL/ATC

The IDDIL/ACT (**I**dentify the assets; **D**efine the attack surface; **D**ecompose the system; **I**dentify attack vectors; **L**ist Threat Actors; **A**nalysis; **T**riage & assessment; **C**ontrols) methodology was published by Lockheed Martin in 2019. It was created by experienced security practitioners in reaction to overly compliance-driven cybersecurity practices which can lead to an unbalanced focus on controls and vulnerabilities, rather than on Threats.

> "Threats cause damage to information systems. Threats utilize vulnerabilities to enact this damage, and security controls are implemented to attempt to prevent or mitigate attacks executed by Threat Actors."[232]

The methodology advocates for adopting the Attacker mindset, and works to provide a method for doing so, and otherwise follows closely a generic Threat Modelling approach.

This involves first decomposing the system into critical data, assets, and the components that interact with it to as much depth as possible (down to the technical implementation and through the lens of their security function). The use of a Data Flow Diagram is recommended for this phase, and covers the first three letters of the IDDIL acronym. Following this, a comprehensive and detailed map of attack paths are identified and categorised (the use of Attack Trees is recommended), before finally determining which Threat sources could traverse these paths and how. To communicate the Threats identified in an organised productive manner, the framework recommends the use of a Threat profile.

The methodology itself describes a very generic Threat Modelling process, generally matching the structure and tool use in the OWASP methodology outlined in an earlier section.

Furthermore, it contains detailed explanations of how the tools used can be integrated into the process (primarily DFD's, attack trees, Threat profiles), with concrete examples of their application. An advantage of the methodology is this high degree of integration with popular Threat Modelling tools, and with Lockheed Martin's own Cyber Kill Chain tool, and that it suggests a so-called 'STRIDE-LM' framework (which usefully adds the 'Lateral Movement' to STRIDE). Therefore, the framework can be used as a helpful reference when creating a Threat Model that would utilise these common tools. The utility of the framework also

lies in its integration of Threat Modelling with other risk management procedures, such as the implementation of controls and performing risk assessments. Finally, there is a useful focus on producing outputs which help document the process such as 'controls scorecard' and 'Threat profiles'.

IDDIL/ATC outlines a powerful and effective approach to Threat Modelling very similar to the OWASP modelling methodology. We prefer OWASP for the purposes of the Data Standards as it is better established and has a strong following and community. However, the Data Standards Threat Modellers would benefit from reading the paper from Muckin et al which introduces this methodology.[233]

10. Attack Lifecycle or Cyber Kill Chain

Attack lifecycle describes this Threat Modelling technique best, as it is the process of dividing a coordinated attack into its constituent stages.

Several frameworks for these stages have existed for a range of fields, with the first cybersecurity focused Attack lifecycle developed by Lockheed Martin in 2011. Since then, several entities (companies, academics, and government organisations) have all designed their own framework for cyber kill chains, separating the stages of a cyber-attack differently. However regardless of the particular Kill Chain framework the general lifecycle of an attack involves first a preparation stage, then a commencement stage where the attack/exploit is conducted/run, and finally an endgame stage after the Attacker has gained access to the system and is achieving their objective. The purpose of Kill Chains is to better understand Attackers' tactics, Threats, and procedures (TTPs) at the various stages identified, so they may be stopped or disrupted during them.

We do not recommend the use of Attack Lifecycle / Cyber Kill Chain in the context of the CDR Threat Modelling because it is not a Threat Modelling framework or methodology. It is extremely low-level, being mostly used to highlight the processes of Attackers and in incident response.

Discussion

The authors of this Report recommend the use of OWASP-TMP as the adopted Threat Modelling methodology, in conjunction with the STRIDE Threat identification framework. As discussed above OWASP-TMP has several features that would benefit Threat Modelling for the CDR. It is considered 'web first' (OWASP being the Open Web Application Security Project), is accepted within the communities of interest, is in active use, and integrates well with other Threat Modelling and risk assessment frameworks. As a Threat classification framework STRIDE is well-established, accepted by government and industry, and can be integrated with OWASP-TMP.

The above recommendation notwithstanding, it is important to note that the most significant factor determining the success of a Threat Modelling activity is not the specific formal methodology adopted. A Threat Modelling methodology is simply a process to help security planners notice and think about things which might otherwise be overlooked. They serve as a construct in which to approach the complex task of understanding key assets, Threats, and mitigations. The most important dimension of carrying out a Threat Modelling activity is in how it is carried out. That the process is done well and with a genuine focus on finding and thoughtfully considering Threats. The "OWASP Threat Modeling Manifesto" articulates the sorts of values and principles which will lead to a high-quality modelling activity.

As can be seen, frameworks are a high-level process, and are, for the most part, aligned. Like most evaluated cybersecurity processes, user engagement is key. To effectively gain from the process, all stages need to be considered in detail which will require expertise - both internal and external. The detail of each stage is important, and ensuring effective and detailed analysis requires in-depth knowledge of the domain areas.

Appendices

Below we set out the general principles we considered for choosing a Threat methodology or framework:

In essence, most Threat Modelling frameworks are consistent with each other. Whilst the classes of Threats change, they are to be adapted and considered by domain experts. Given the common elements between different Threat Modelling processes, it is possible to run multiple processes simultaneously or together. This would allow for multiple communities to easily interpret and accept findings, as some processes are more accepted than others. The OWASP-TMP processes, for example, can integrate with STRIDE or OCTAVE.

As the CDR is at the nexus of the Australian government requirements, the choice of Threat Modelling methodology should incorporate this. Similarly, the CDR has strong ties with Open Banking across several countries and jurisdictions, and integration and consistency with this community is also to be considered. The CDR environments are externally owned and operated, cloud-first, and based on APIs. The majority of the environment is in the communication processes and structures.

The focus should be on Threat sources specific to the types of Threats applicable to the CDR platforms. These are different from many common paradigms. Existing literature and guidelines on Threat Modelling have largely been focused towards well-established domains such as critical digital infrastructure, financial banking, and web-specific systems.[234] Therefore, these guidelines will not directly relate to the CDR because of its unique characteristics, such as decentralisation, and high customer and third-party involvement. Nevertheless, the general approaches, Threat types, security risk management processes and countermeasures will be similar and should be undertaken in alignment with existing Threat Modelling guidance.

As such, when working on the common early stages of the Threat Modelling process – identifying Threats and techniques that could be applied against key infrastructure – it is important to ensure a wide variety of applicable sources are consulted. These may include frameworks including the Mitre ATT&CK framework, the OWASP Web Security Testing Framework,[235] and the NIST Cybersecurity Framework. These low-level processes articulate individual Threats and considerations at a much more granular level.

Threat Modelling is also closely linked to risk assessment, and the outcomes of Threat Modelling should inform work in this space. Some Threat Modelling processes are complementary to risk management processes (see UNSW Risk Report), and others can be superseded by the more detailed structures and processes risk management affords. For example, phase three of the OWASP-TMP aims to provide appropriate countermeasures for listed Threats – something that is conducted in a more detailed and structured way within a full RMF. Whilst adapting existing frameworks is often outside of best practice, it is generally accepted to defer stages to an appropriately designed process. For example, the third OWASP-TMP stage could be completed in conjunction with a more comprehensive risk management process.

Appendix C: Threat Modelling Tools and Techniques

Attack Trees
Attack trees are a method of organising Threats scenarios and their related attack paths to help recognise new paths and determine countermeasures to identified paths. All paths that are without countermeasures are vulnerabilities to which the organisation or system is exposed. In this methodology, tree leaves are in the form of boxes, often with the boxes coloured under a colour coding scheme. The tree is constructed going from top to bottom.

- Possible Threats are at the root (top) of a tree, often coloured in white.
- Explored attack paths for each Threat are identified next, often coloured in orange.
- Countermeasures for each attack path, where possible are listed below, often coloured in green

Data Flow Diagrams
These are a class of block diagrams that show how data in the system flows, where it is processed and modified, stored, and who has access to it. The access privileges (trust levels) of data may change as it moves from one system component to another, and this must be included as well, with a data arrow shown crossing a privilege boundary.

DRDC's Threat Characterization Framework
This framework aims to provide a structured representation of Threats by organising all information about the Threat into the categories: adversary (the Threat source), attack (the method used to cause harm), asset (the resource to be acquired/the Attacker objective), and effect (the impact of the attack on the organisation). Each of these information categories are further divided to create a holistic representation of the Threat. This method of Threat categorisation captures and structures all relevant aspects of a Threat, and is worth incorporating into the Threat Model as an additional tool to guide the process.

OWASP Threat Model Cookbook
This tool is a collection of Threat Models submitted by users to a GitHub repository. Born out of a lack of real-life Threat Models used in industry, the repository contains Attack Trees, data flow diagrams, and a more detailed Threat Modelling case study. While this tool may not directly help the Threat Modelling process, it can be used to inform what potential diagrams in the Threat Model might look like, and can provide inspiration for prototype diagrams at the start of the process.

Threat Profiles
A Threat profile is a tabular representation of all Threats and their corresponding attributes, meant to communicate the Threats identified after Threat Modelling in a condensed, organised manner. Typically, the major Threat attributes include the Threat's name, type (defined by STRIDE, ATT&CK tactics, etc.), attack surface exploited, tactics and techniques utilised, source, consequence, the vulnerabilities the Threat exploits, and the potential controls that might mitigate the risk of the Threat.

Appendices

Appendix D: Business Impact Levels

PSPF Policy 8 sets out a Business Impact Levels (**BIL**) tool for assessment of the level of impact from compromised information, taking into account damage to the national interest, organisations or individuals.

In the context of an RMF, the BIL tool helps analyse of consequences that would follow on a risk being realised. In particular, it can be used to assess the impact of compromise of sensitive information, taking into account damages to the national interest, organisations, or individuals. The use of the BIL tool in the context of an RMF is discussed further in the UNSW Risk Report.

Business Impact Levels are in Table 1 of PSPF Policy 8:

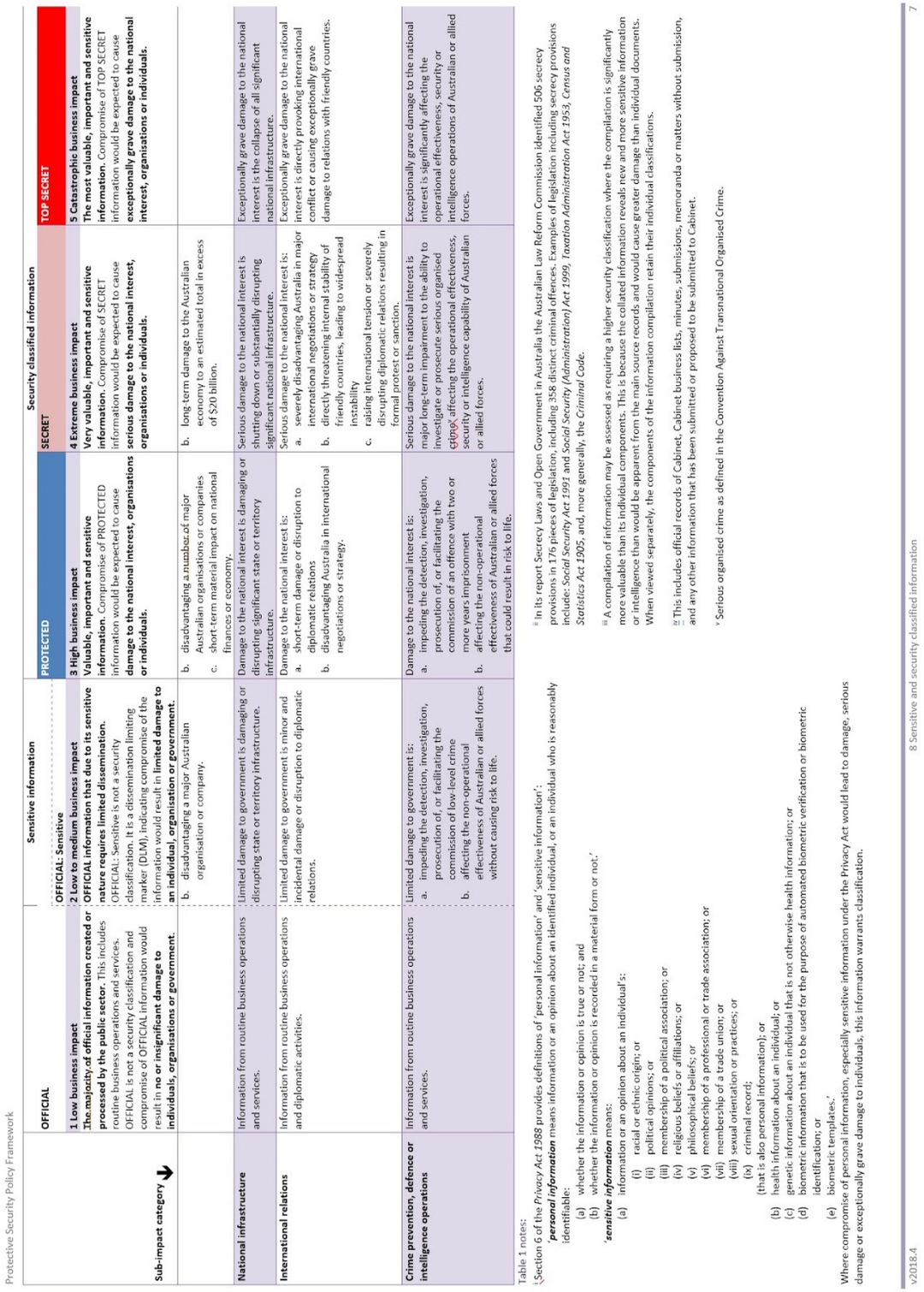
Protective Security Policy Framework

Table 1 Business Impact Levels tool – Assessing damage to the national interest, government, organisations or individuals

		Sensitive information	Security classified information		
	OFFICIAL		**PROTECTED**	**SECRET**	**TOP SECRET**
		OFFICIAL: Sensitive			
	1 Low business impact	**2 Low to medium business impact**	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
Sub-impact category ↓	**The majority of official information created or processed by the public sector.** This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination.** OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in **limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information.** Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
Potential impact on individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. Includes personal information as defined in the *Privacy Act*. This may include information (or an opinion) about an identifiable individual (eg, members of the public, staff etc) but would not include information defined as sensitive information under the *Privacy Act*.	Limited damage to an individual is: a. potential harm, for example injuries that are not serious or life threatening or b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is **not life threatening**.	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially **significant harm or potentially life threatening injury**.	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to **directly threaten or lead to the loss of life of an individual or small group**.	Exceptionally grave damage is: a. widespread loss of life b. discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.
Potential impact on organisations from compromise of the information					
Entity operations, capability and service delivery	Information from routine business operations and services.	Limited damage to entity operations is: a. a degradation in organisational capability to an extent and duration that, while the **entity can perform its primary functions**, the effectiveness of the functions is noticeably reduced b. minor loss of confidence in government.	Damage to entity operations is: a. a degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform one or more of its primary functions** b. major loss of confidence in government.	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform any of its functions** b. directly threatening the internal stability of Australia.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Entity assets and finances, eg, operating budget	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to $**10 million to $100 million**.	Damage is: a. substantial financial loss to an entity b. **$100 million to $10 billion** damage to entity assets.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Legal compliance, eg, information compromise would cause non-compliance with legislation,[ii] commercial confidentiality or legal professional privilege	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal professional privilege for communications between legal practitioners and their clients b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation resulting in less than two years' imprisonment.	Damage is: a. failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.
Aggregated data[iii]	An aggregation of routine business information.	A significant aggregated holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.
Potential impact on government or the national interest from compromise of the information					
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher business impact level).	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a. impeding the development or operation of major policies b. revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet[iv] (not otherwise captured by higher level business impacts).	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.
Australian economy	Information from routine business operations and services.	Limited damage to government is: a. undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies	Damage to the national interest is: a. undermining the financial viability of a major Australian-based or owned organisation or company	Serious damage to the national interest is: a. undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector)	Exceptionally grave damage to the national interest is the collapse of the Australian economy.

v2018.4 8 Sensitive and security classified information 6

FOR PUBLIC RELEASE



Protective Security Policy Framework

Sub-impact category →	Security classified information			
	OFFICIAL	PROTECTED	SECRET	TOP SECRET
	OFFICIAL: Sensitive	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
	1 Low business impact	**Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information.** Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
	2 Low to medium business impact	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
	OFFICIAL information that due to its sensitive nature requires limited dissemination. OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in **limited damage to an individual, organisation or government.**	**OFFICIAL is official information created or processed by the public sector.** This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**		
	Information from routine business operations and services.	Limited damage to government is damaging or disrupting state or territory infrastructure. b. disadvantaging a major Australian organisation or company.	Serious damage to the national interest is shutting down or substantially disrupting significant national infrastructure. b. long-term damage to the Australian economy to an estimated total in excess of $20 billion.	Exceptionally grave damage to the national interest is the collapse of all significant national infrastructure.
National infrastructure	Information from routine business operations and diplomatic activities.	Limited damage to government is minor and incidental damage or disruption to diplomatic relations.	Serious damage to the national interest is: a. severely disadvantaging Australia in major international negotiations or strategy b. directly threatening internal stability of friendly countries, leading to widespread instability c. raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	Exceptionally grave damage to the national interest is directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries.
International relations	Information from routine business operations and services.	Limited damage to government is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime b. affecting the non-operational effectiveness of Australian or allied forces without causing risk to life.	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime[iv] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage to the national interest is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.
Crime prevention, defence or intelligence operations	Information from routine business operations and services.	Limited damage to government is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime b. affecting the non-operational effectiveness of Australian or allied forces without causing risk to life.	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime[iv] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage to the national interest is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.

Table 1 notes:

[i] Section 6 of the *Privacy Act 1988* provides definitions of 'personal information' and 'sensitive information':

'***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not.'

'***sensitive information*** means:

(a) information or an opinion about an individual's:
  (i) racial or ethnic origin; or
  (ii) political opinions; or
  (iii) membership of a political association; or
  (iv) religious beliefs or affiliations; or
  (v) philosophical beliefs; or
  (vi) membership of a professional or trade association; or
  (vii) membership of a trade union; or
  (viii) sexual orientation or practices; or
  (ix) criminal record;
  (that is also personal information); or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates.'

Where compromise of personal information, especially sensitive information under the Privacy Act would lead to damage, serious damage or exceptionally grave damage to individuals, this information warrants classification.

[ii] In its report Secrecy Laws and Open Government in Australia the Australian Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences. Examples of legislation including secrecy provisions include: *Social Security Act 1991* and *Social Security (Administration) Act 1999, Taxation Administration Act 1953, Census and Statistics Act 1905*, and, more generally, the *Criminal Code*.

[iii] A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

[iv] This includes official records of Cabinet, Cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to Cabinet.

[v] Serious organised crime as defined in the Convention Against Transnational Organised Crime.

v2018.4

Endnotes

[1]Coen Teunissen, Isabella Voce and Russell Smith, 'Estimating the cost of pure cybercrime to Australian individuals', Statistical Bulletin No 34 (2021), Canberra: Australian Institute of Criminology, https://www.aic.gov.au/publications/sb/sb34.

[2]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020).

[3]Threat Modeling Process, https://owasp.org/www-community/Threat_Modeling_Process. Supporting commentary available at https://www.threatmodelingmanifesto.org/.

[4]Tong Xin, and Ban Xiaofang, 'Online banking security analysis based on STRIDE Threat Model' (2014) 8.2 International Journal of Security and Its Applications 271-282.

[5]N Biddle, B Edwards, M Gray and S McEachern, 'Public attitudes towards data governance in Australia', CSRM Working Paper No 12/2018.

[6]Australian Government Department of Home Affairs, Cyber and Infrastructure Security Centre, Legislative information and reforms, https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure.

[7]Australian Government Attorney-General's Department, Review of the Privacy Act 1988, https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.

[8]ACCC, Digital Platforms Inquiry: Final Report (June 2019) Ch 7.

[9]Australian Government, Ransomware Action Plan (October 2021), https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf.

[10]Australian Government, National Data Security Action Plan: Discussion paper – A call for views (2021), https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf.

[11]Australian Government, Strengthening Australia's cyber security regulations and incentives – A call for views (2021), https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf.

[12]Joseph Brookes, 10-year cyber strategy to be recast by Labor, InnovationAus (19 August 2022), https://www.innovationaus.com/10-year-cyber-strategy-to-be-recast-by-labor/.

[13]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020).

[14]HB 167-2006 Security risk management, Definitions and glossary.

[15]*Competition and Consumer Act 2019* (Cth) (**CCA**) Pt IVD Div 3.

[16]Lyria Bennett Moses, Katharine Kemp, Peter Leonard, Rob Nicholls, *Risk Management for the Consumer Data Standards: A report to the Data Standards Chair* (UNSW, 2022) ("UNSW Risk Report").

[17]CCA s 56AC.

[18]CCA s 56AA.

[19]CCA Pt IVD Div 5. The Privacy Safeguards largely replace the Australian Privacy Principles (APPs) from the Privacy Act 1988 (Cth) in respect of Data Holders' and ADRs' dealings with CDR data: CCA s 56EC.

[20]CCA s 56BA; more generally CCA Pt IVD Div 2A.

[21]CCA s 56FA.

[22]CCA s 56FA.

[23]Each of which is described more fully in the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

[24]CCA ss 56AK, 56CA.

[25]CDR Rules 1.10A; 7.5.

[26]*Privacy Act 1988* (Cth) Pt IIIC.

[27]This is evident in the Protective Security Policy Framework (PSPF) Policy 3.

[28]NIST Special Publication 800-37 rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, https://doi.org/10.6028/NIST.SP.800-37r2. Note that this publication uses the term "information life cycle".

[29]See, for example, BBC News, Patient data found on hard drives (7 May 2009), https://news.bbc.co.uk/2/hi/uk_news/scotland/glasgow_and_west/8037355.stm.

[30]CCA s 56FA.

[31]CDR Rule 8.11(1)(c)(iv).

Endnotes

[32]Chris Culnane, Benjamin IP Rubinstein and Vanessa Teague, 'Health Data in an Open World' arXiv: 1712.05627, https://doi.org/10.48550/arXiv.1712.05627.

[33]Christine O'Keefe et al, 'The De-identification Decision-making Framework' (CSIRO Data61, 18 September 2017), https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS1.

[34]Chris Culnane, Benjamin IP Rubinstein and Vanessa Teague, 'Health Data in an Open World' arXiv: 1712.05627, https://doi.org/10.48550/arXiv.1712.05627.

[35]Australian Government, Consumer Data Right, How it works, https://www.cdr.gov.au/how-it-works.

[36]Charles Perrow, Normal Accidents: Living with High Risk Technologies (Princeton University Press, updated edition, 1999).

[37]Crowdstrike adversary universe, Wizard Spider, https://adversary.crowdstrike.com/en-US/adversary/wizard-spider/.

[38]Paul Reynolds, 'Wizard Spider': Who are they and how do they operate? (RTE, 19 May 2021), https://www.rte.ie/news/crime/2021/0518/1222349-ransomware-crime-group/.

[39]Wikipedia, Office of Personnel Management data breach, https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach.

[40]Conor Lally, Wizard Spider profile: Suspected gang behind HSE attack is part of world's first cyber-cartel (Irish Times, 18 May 2021), https://www.irishtimes.com/news/crime-and-law/wizard-spider-profile-suspected-gang-behind-hse-attack-is-part-of-world-s-first-cyber-cartel-1.4568806.

[41]PSPF Policy 8 Table 1 Business Impact Levels tool – Assessing damage to the national interest, government, organisations or individuals; see Appendix D.

[42]PSPF Policy 8 Table 1 Business Impact Levels tool – Assessing damage to the national interest, government, organisations or individuals; see Appendix D.

[43]Tom Lamont, Life after the Ashley Madison affair (The Guardian, 28 February 2016), https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked.

[44]'Department of Home Affairs, Ransomware Action Plan (2021), https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf (the "Australian Government does not condone ransom payments being made to cybercriminals"). ACSC, Ransomware, https://www.cyber.gov.au/ransomware ("Never pay a ransom").

[45]Lally n 40.

[46]Mandiant, 'M-Trends 2022: Mandiant Special Report', https://www.mandiant.com/m-trends (account required).

[47]'See as an example the Attack Motivation Vocabulary identified under the Structured Threat Information Expression (STIX™) cyber threat intelligence framework.

[48]Paul Lipman, 'Why Nation-State Hacking Should Matter to Everyone' (22 June 2018), https://www.forbes.com/sites/forbestechcouncil/2018/06/22/why-nation-state-hacking-should-matter-to-everyone/?sh=44ebc82413ec.

[49]HP Wolf Security, The Best Offense is Good Defense: Endpoint Protection Strategies (12 June 2021), https://www.csoonline.com/article/3621774/nation-states-cyberconflict-and-the-web-of-profit.html.

[50]Vasu Jakkal, How nation-state attackers like NOBELIUM are changing cybersecurity (28 September 2021), https://www.microsoft.com/security/blog/2021/09/28/how-nation-state-attackers-like-nobelium-are-changing-cybersecurity/.

[51]ACSC, Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services (8 May 200), https://www.cyber.gov.au/acsc/view-all-content/alerts/advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services.

[52]Lance Spitzner, Nation State Threat Actors: From a Security Awareness Perspective (15 February 2022), https://www.sans.org/blog/nation-state-threat-actors-from-a-security-awareness-perspective/.

[53]Lance Spitzner, Nation State Threat Actors: From a Security Awareness Perspective (15 February 2022), https://www.sans.org/blog/nation-state-threat-actors-from-a-security-awareness-perspective/.

[54]Lance Spitzner, Nation State Threat Actors: From a Security Awareness Perspective (15 February 2022), https://www.sans.org/blog/nation-state-threat-actors-from-a-security-awareness-perspective/.

[55]Lance Spitzner, Nation State Threat Actors: From a Security Awareness Perspective (15 February 2022), https://www.sans.org/blog/nation-state-threat-actors-from-a-security-awareness-perspective/.

[56]Cyber Cube, 'Understanding Criminal Cyber Threat Actors and Motivations', https://www.actuarialpost.co.uk/downloads/cat_1/CyberCube%202022%20Understanding%20criminal%20cyber%20threat%20actors%20and%20motivations.pdf.

[57]David Wroe, China 'behind' huge ANU hack amid fears government employees could be compromised, SMH (5 June 2019), https://www.smh.com.au/politics/federal/china-behind-huge-anu-hack-amid-fears-government-employees-could-be-compromised-20190605-p51uro.html.

[58]Trellix Global Threat Research, In the Crosshairs: Organizations and Nation State Cyber Threats, https://www.trellix.com/en-us/assets/docs/trellix-csis-organizations-and-nation-state-cyber-threats-report.pdf.

[59]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[60]ACSC Annual Cyber Threat Report 2020-21, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.

[61]Trellix Global Threat Research, In the Crosshairs: Organizations and Nation State Cyber Threats, https://www.trellix.com/en-us/assets/docs/trellix-csis-organizations-and-nation-state-cyber-threats-report.pdf.

[62]Cybersecurity & Infrastructure Security Agency (CISA), Alert AA22-110A, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

[63]National Security Agency et al, Cybersecurity Advisory, Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments (July 2021), https://media.defense.gov/2021/jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.

[64]Cybersecurity & Infrastructure Security Agency (CISA), IR-ALERT-H-16-056-01, https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

[65]Reuters, US ties North Korean hacker group Lazaras to huge cryptocurrency theft (15 April 2022), https://www.reuters.com/technology/us-ties-north-korean-hacker-group-lazarus-huge-cryptocurrency-theft-2022-04-14/.

[66]US Department of the Treasury, Press Releases, US Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats (6 May 2022), https://home.treasury.gov/news/press-releases/jy0768.

[67]Andrew Higgins, Lithuania blames Russia for cyberattacks, citing threats over cargo restrictions (27 June 2022), https://www.nytimes.com/2022/06/27/world/europe/lithuania-russia-cyberattacks.html.

[68]The Associated Press, Cyberattack hits Lithuania after sanctions feud with Russia (27 June 2022), https://abcnews.go.com/International/wireStory/cyberattack-hits-lithuania-sanctions-feud-russia-85787252.

[69]ACSC, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure.

[70]Annie Fixler, 'The Cyber Threat from Iran after the Death of Soleimani' (2020) 13(2) CTC Sentinel, https://ctc.usma.edu/cyber-threat-iran-death-soleimani/.

[71]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[72]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[73]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[74]Security Staff, 'Deepfakes, cyber extortion, API attacks and other emerging cyber threats' Security Magazine (8 August 2022), https://www.securitymagazine.com/articles/98127-deepfakes-cyber-extortion-api-attacks-and-other-emerging-cyber-threats.

[75]Wallarm, API Vulnerabilities Discovered and Exploited in Q1-2022, https://www.wallarm.com/resources/api-vulnerabilities-discovered-and-exploited-in-q1-2022.

[76]Salt Security, State of API Security, https://salt.security/press-releases/salt-security-state-of-api-security-report-reveals-api-attacks-increased-681-in-the-last-12-months#:~:text=The%20State%20of%20API%20Security%20Report%20pulls%20from,to%20a%20321%25%20increase%20in%20overall%20API%20traffic.

[77]ACSC, Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services (8 May 200), https://www.cyber.gov.au/acsc/view-all-content/alerts/advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services.

[78]NIST Computer Security Resource Center, Advanced Persistent Threat (APT), https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

[79]NIST Computer Security Resource Center, Advanced Persistent Threat (APT), https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

[80]Crowdstrike, Advanced Persistent Threat (APT) (15 June 2022), https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

[81]NSA and FBI Cybersecurity Advisory, Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware (August 2020 rev 1), https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF.

[82]'Indictment, USA v Aleksei Sereyevich Morenets et al, Criminal No 18-263, US District Court Western District Pennsylvania, https://www.justice.gov/opa/page/file/1098481/download.

Endnotes

[83]Andrea Peterson, Everything you need to know abou the alleged Chinese military hacker squad the US just indicted, Washington Post (19 May 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/05/19/everything-you-need-to-know-about-the-alleged-chinese-military-hacker-squad-the-u-s-just-indicted/.

[84]Christian Espinosa, The Secure Blog, Top 10 Organized Cybercrime Syndicates, https://christianespinosa.com/blog/top-10-organized-cybercrime-syndicates/.

[85]Australian Institute of Criminology, Statistical Bulletin 34 (July 2021), https://www.aic.gov.au/sites/default/files/2021-07/sb34_estimating_the_cost_of_pure_cybercrime_to_australian_individuals.pdf.

[86]Max Mason, More than half of Australian businesses disrupted by cyber attacks (23 April 2021), https://www.afr.com/policy/foreign-affairs/more-than-half-of-australian-businesses-disrupted-by-cyber-attacks-20210423-p57lvs.

[87]Bishopfox, Organized: The Kingpins of Cybercrime, https://bishopfox.com/blog/kingpins-cybercrime.

[88]Christian Espinosa, The Secure Blog, Top 10 Organized Cybercrime Syndicates, https://christianespinosa.com/blog/top-10-organized-cybercrime-syndicates/.

[89]Imperva, Magecart, https://www.imperva.com/learn/application-security/magecart/.

[90]TechTarget, Evil Corp, https://www.techtarget.com/searchsecurity/definition/Evil-Corp.

[91]ACSC, Annual Cyber Threat Report 1 July 2020 to 30 June 2021, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.

[92]Cequence Security, 'Ulta Beauty Reduces Costs by Blocking API-based Enumeration Attacks' (3 August 2022), https://www.cequence.ai/blog/ulta-beauty-reduces-costs-by-blocking-api-based-enumeration-attacks/.

[93]See Betsy Amy-Vogt 'Cequence Security finds the hidden APIs that open companies to cyberthreats and traditional crime' Silicon Angle (23 August 2022), https://siliconangle.com/2022/08/23/cequence-security-finds-the-hidden-apis-that-open-companies-to-cyberthreats-and-traditional-crime-awsshowcases2e4/.

[94]ID Care, Understanding Identity Theft, https://www.idcare.org/fact-sheets/understanding-identity-theft.

[95]ID Care, Understanding Identity Theft, https://www.idcare.org/fact-sheets/understanding-identity-theft.

[96]Bitsight, Ransomware: The Rapidly Evolving Trend, https://www.bitsight.com/sites/default/files/migration/documents/Ransomware_The%2520Rapidly%2520Evolving%2520Trend.pdf.

[97]Australian Government, Consumer Data Right, Become an Accredited Data Recipient, https://www.cdr.gov.au/for-providers/become-accredited-data-recipient.

[98]Trend Micro Ransomware report Q1 2022, https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf.

[99]Australian Taxation Office, Organised crime, https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Organised-crime/.

[100]Australian Criminal Intelligence Commission, Key Enablers, Organised Crime in Australia 2017, https://www.acic.gov.au/sites/default/files/2020-08/oca_2017_key_enablers.pdf.

[101]Australian Institute of Criminology, Trends & issues in crime and criminal justice, No 565 (December 2018), https://www.aic.gov.au/sites/default/files/2020-05/exploring_the_relationship_between_organised_crime_and_volume_crime_071218.pdf.

[102]Australian Criminal Intelligence Commission, Organised Crime in Austraila 2017, https://www.acic.gov.au/sites/default/files/2020-08/oca_2017_230817_1830.pdf.

[103]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[104]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[105]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[106]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[107]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[108]See for example the financial and corporate harms experienced by LandMark White following a 2019 cybersecurity incident detailed in Julian Bajkowski, 'Massive data breach costs valuer LandMark White $7m', IT News (6 May 2019), https://www.itnews.com.au/news/massive-data-breach-costs-valuer-landmark-white-7m-524716.

[109]See for example *Compulife Software Inc v Newman*, 959 F.3d 1288 (11th Cir. 2020).

[110]*Compulife Software Inc v Newman*, 959 F.3d 1288 (11th Cir. 2020).

[111]Paayal Zaveri, 'Unsealed letter in Uber-Waymo case details how Uber employees allegedly stole trade secrets', CNBC (15 December 2017, https://www.cnbc.com/2017/12/15/jacobs-letter-in-uber-waymo-case-says-uber-staff-stole-trade-secrets.html.

[112]Lyle Adriano, 'Uber hacked its competitors, ex-manager alleges', Insurance Business America (18 December 2017), https://www.insurancebusinessmag.com/us/news/cyber/uber-hacked-its-competitors-exmanager-alleges-87949.aspx.

[113]See, for example, *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496.

[114]See, for example, Privacy Act 1988 Sch 1 APP 9 and the Privacy Safeguards under CCA Part IVD.

[115]See for example the discussion in Christine Wong et al, HSF Insight Legal Briefings, 'Litigation Risks Arising from Cyber Attacks / Data Breach Incidents' (15 March 2022), https://www.herbertsmithfreehills.com/insight/litigation-risks-arising-from-cyber-attacksdata-breach-incidents

[116]See for example *Evans v Health Administration Corporation* [2019] NSWSC 1781.

[117]ACS, Cybersecurity: Threats Challenges Opportunities (November 2016), https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf.

[118]A 2015 survey undertaken by Kaspersky Lab found that 12% of businesses hit by a DDoS attack worldwide were confident the attacks had been caused by a competitor, see Kaspersky Lab, Denial of Service: How Businesses Evaluate the Threat of DDoS Attacks IT Security Risks Special Report Series https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234158/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf.

[119]Josh Fruhlinger, CSO Online, 'DDoS Attacks: Definition, examples, and techniques' (31 January 2022) https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html.

[120]BBC News, 'Amazon 'thwarts largest ever DDoS cyber-attack'' (18 June 2020) https://www.bbc.com/news/technology-53093611.

[121]See for example the discussion contained Carl Colwill, 'Human factors in information security: The insider threat-Who can you trust these days?' 2009 14(4) Information Security Technical Report 186-196, https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/Previous%20Articles/Ch11InternalThreatsUsers.pdf.

[122]In this context, the focus on behaviours that directly impact cybersecurity, rather than other kinds of business harms, such as harassment, lost productivity, workplace violence, or adverse culture.

[123]McKinsey & Co, 'Insider threat: The human element of cyberrisk' (September 2018), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/insider-threat-the-human-element-of-cyberrisk.

[124]See the discussion on insider vulnerabilities in N Khan et al, 'Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks' (2022) 24 Cognition, Technology & Work 393–421, https://doi.org/10.1007/s10111-021-00690-z.

[125]See for examples the discussions by Maureen Data Systems at https://www.mdsny.com/motive-doesnt-matter-the-three-types-of-insider-threats and SISA Information Security at https://www.mdsny.com/motive-doesnt-matter-the-three-types-of-insider-threats/.

[126]Cybersecurity and Infrastructure Security Agency (CISA), Insider Threat Mitigation Guide (November 2020), https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.

[127]ProofPoint, The Primary Factors Motivating Insider Threats (17 September 2019), https://www.proofpoint.com/us/blog/insider-threat-management/primary-factors-motivating-insider-threats.

[128]See Kate Conger, 'Ex-Amazon Worker Convicted in Capital One Hacking' NY Times (17 June 2022), https://www.nytimes.com/2022/06/17/technology/paige-thompson-capital-one-hack.html.

[129]Kate Conger, 'Ex-Amazon Worker Convicted in Capital One Hacking' NY Times (17 June 2022), https://www.nytimes.com/2022/06/17/technology/paige-thompson-capital-one-hack.html. See further Rob McLean, 'A hacker gained access to 100 million Capital One credit card applications and accounts', CNN Business (30 July 2019), https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html.

[130]Fahmida Rashid, 'Capital One Breach Highlights Challenges of Insider Threats', Decipher (30 July 2019), https://duo.com/decipher/capital-one-breach-highlights-challenges-of-insider-threats.

[131]John MacFarlane, 4.2 million Desjardins members affected by a breach, credit union now says, CBC (1 November 2019), https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216.

[132]John MacFarlane, 4.2 million Desjardins members affected by a breach, credit union now says, CBC (1 November 2019), https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216.

[133]Becky Bracken, OpenSea NFT Marketplace Faces Insider Hack, DarkReading (2 July 2022), https://www.darkreading.com/vulnerabilities-threats/opensea-nft-marketplace-faces-insider-hack.

Endnotes

[134]Becky Bracken, OpenSea NFT Marketplace Faces Insider Hack, DarkReading (2 July 2022), https://www.darkreading.com/vulnerabilities-threats/opensea-nft-marketplace-faces-insider-hack.

[135]Helen Christoph, Google Claims Uber Swiped Self-Driving Car Technology, Courthouse News Service (27 February 2017), https://www.courthousenews.com/google-claims-uber-swiped-self-driving-car-technology/.

[136]K2 Enterprises, Insider Threats – The Worst Data Breaches Caused By Malicious Insiders, https://www.k2e.com/articles/insider-threats/.

[137]Jessica Davis, 'Anthem: Insider theft exposes data of 18,000 Medicare members, Healthcare IT News (31 July 2017), https://www.healthcareitnews.com/news/anthem-insider-theft-exposes-data-18000-medicare-members.

[138]Jessica Davis, 'Anthem: Insider theft exposes data of 18,000 Medicare members, Healthcare IT News (31 July 2017), https://www.healthcareitnews.com/news/anthem-insider-theft-exposes-data-18000-medicare-members.

[139]Bishr Tabbaa, 'Take Out – How Anthem was Breached', Medium (17 February 2019), https://medium.com/dataseries/take-out-how-anthem-was-breached-276b9ffca8da.

[140]Ricardo Lara, California Department of Insurance, Anthem Data Breach, https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm.

[141]Terry Ray, Motive doesn't atter: The three types of insider threats, BetaNews, https://www.mdsny.com/motive-doesnt-matter-the-three-types-of-insider-threats/.

[142]Juliana De Groot, 'Social Engineering Attacks: Common Techniques& How to Prevent an Attack', Digital Guardian (14 March 2022), https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

[143]Terry Ray, Motive doesn't atter: The three types of insider threats, BetaNews, https://www.mdsny.com/motive-doesnt-matter-the-three-types-of-insider-threats/.

[144]Zack Whittaker, 'A hacker used Twitter's own 'admin' tool to spread cryptocurrency scam', TechCrunch (16 July 2020), https://techcrunch.com/2020/07/15/twitter-hacker-admin-scam/.

[145]Zack Whittaker, 'A hacker used Twitter's own 'admin' tool to spread cryptocurrency scam', TechCrunch (16 July 2020), https://techcrunch.com/2020/07/15/twitter-hacker-admin-scam/.

[146]Exabeam, What is an insider threat? Understand the Problem and Discover 4 Defensive Strategies, https://www.exabeam.com/explainers/insider-threat/insider-threats/.

[147]Juliana De Groot, 'Social Engineering Attacks: Common Techniques& How to Prevent an Attack', Digital Guardian (14 March 2022), https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

[148]Terry Ray, Motive doesn't atter: The three types of insider threats, BetaNews, https://www.mdsny.com/motive-doesnt-matter-the-three-types-of-insider-threats/.

[149]'Terry Ray, Motive doesn't atter: The three types of insider threats, BetaNews, https://www.mdsny.com/motive-doesnt-matter-the-three-types-of-insider-threats/.

[150]'Tim Conkle, 'The Human Element of Cybersecurity', Forbes (24 January 2020), https://www.forbes.com/sites/forbestechcouncil/2020/01/24/the-human-element-of-cybersecurity/?sh=bc8c13832933.

[151]OAIC, Notifiable Data Breaches Report: July-December 2021 (22 February 2022), https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021.

[152]Clare Stouffer, Hacktivism: An overview plus high-profile groups and examples', Norton (8 September 2021), https://us.norton.com/blog/emerging-threats/hacktivism.

[153]Cyber Cube, 'Understanding Criminal Cyber Threat Actors and Motivations', https://www.actuarialpost.co.uk/downloads/cat_1/CyberCube%202022%20Understanding%20criminal%20cyber%20threat%20actors%20and%20motivations.pdf.

[154]SentinelOne, What is Hacktivism?, https://www.sentinelone.com/cybersecurity-101/hacktivism/.

[155]Patrick Putman, 'Script Kiddie: Unskilled Amateur or Dangerous Hackers?', US Cybersecurity Magazine https://www.uscybersecurity.net/script-kiddie/.

[156]Cyber Cube, 'Understanding Criminal Cyber Threat Actors and Motivations', https://www.actuarialpost.co.uk/downloads/cat_1/CyberCube%202022%20Understanding%20criminal%20cyber%20threat%20actors%20and%20motivations.pdf.

[157]Cyber Cube, 'Understanding Criminal Cyber Threat Actors and Motivations', https://www.actuarialpost.co.uk/downloads/cat_1/CyberCube%202022%20Understanding%20criminal%20cyber%20threat%20actors%20and%20motivations.pdf.

[158]Associated Press, Cyberattack Forces Iran Steel Company to Halt Production, Security Week (27 June 2022), https://www.securityweek.com/cyberattack-forces-iran-steel-company-halt-production.

[159]Associated Press, Cyberattack Forces Iran Steel Company to Halt Production, Security Week (27 June 2022), https://www.securityweek.com/cyberattack-forces-iran-steel-company-halt-production.

[160]Bruce Schneier, 'Attack trees: Modeling security threats,' Dr. Dobb's Journal (December 1999).

[161]Wenjun Xiong and Robert Lagerström, 'Threat Modeling–A systematic literature review' (2019) 84 *Computers & Security* 53-69.

[162]David B Fox, et al, Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions: Threat Model ATT and CK/CAPEC Version, MITRE (2018), https://www.mitre.org/sites/default/files/2021-11/prs-18-1725-ngci-enhanced-cyber-threat-model-for-financial-services-sector-institutions.pdf.

[163]Risk Policy Element Five.

[164]Risk Policy Element Seven.

[165]Australian Government Department of Finance, Comcover Information Sheet, Understanding and Managing Shared Risk (2016).

[166]PSPF Policy 3, C.1.

[167]PSPF Policy 3, C.2..

[168]Australian Cyber Security Centre, Guidelines for Software Development, https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-software-development.

[169]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020).

[170]See https://owasp.org/www-project-application-security-verification-standard/.

[171]Victoria Drake, Threat Modelling (OWASP), https://owasp.org/www-community/Threat_Modeling.

[172]Larry Conklin, Threat Modelling Process (OWASP), https://owasp.org/www-community/Threat_Modeling_Process.

[173]The Threat Modeling Manifesto is available at https://www.threatmodelingmanifesto.org.

[174]OWASP Threat Modeling Process, https://owasp.org/www-community/Threat_Modeling_Process.

[175]OWASP Top 10, https://owasp.org/www-project-top-ten/.

[176]Michael Muckin and Scott C Fitch, A Threat-Driven Approach to Cyber Security (Lockheed Martin Corporation, 2019), https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf).

[177]Microsoft Threat Modeling Tool threats (25 August 2022), https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

[178]Tong Xin and Ban Xiaofang. 'Online banking security analysis based on STRIDE Threat Model' (2014) 8.2 International Journal of Security and Its Applications 271-282.

[179]ACSC, Cyber Incident Management Arrangements for Australian Governments, https://www.cyber.gov.au/sites/default/files/2019-03/cima_2018_A4.pdf.

[180]HB 167-2006 Security risk management, Definitions and glossary.

[181]ACSC, Malware, https://www.cyber.gov.au/acsc/view-all-content/threats/malware#:~:text=Malware%20%28short%20for%20%27malicious%20software%27%29%20is%20software%20that,program%20that%20is%20used%20for%20a%20malicious%20purpose.

[182]Isabelle Voce and Anthony Moran, 'Ransomware victimisation among Australian computer users, Statistical Bulletin 35, https://www.aic.gov.au/sites/default/files/2021-10/sb35_ransomware_victimisation_among_australian_computer_users.pdf.

[183]Homeland Security, Malware Trends (October 2016), https://www.cisa.gov/uscert/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf

[184]Homeland Security, Malware Trends (October 2016), https://www.cisa.gov/uscert/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf.

[185]Sam Cook, Comparitech, Malware statistics and facts for 2022 (3 July 2022), https://www.comparitech.com/antivirus/malware-statistics-facts/.

[186]Security Boulevard, What is a DDoS Attack? (3 August 2022), https://securityboulevard.com/2022/08/what-is-a-ddos-attack/.

[187]Security Boulevard, What is a DDoS Attack? (3 August 2022), https://securityboulevard.com/2022/08/what-is-a-ddos-attack/.

[188]Yağmur Şahin, 'How GitHub Survived the Biggest DDoS Attack Ever Recorded?' (Medium, 6 November 2021) https://medium.com/technology-hits/how-github-survived-the-biggest-ddos-attack-ever-recorded-6907ba6f5c98#:~:text=On%20February%2028%2C%202018%2C%20Github%20was%20the%20victim,attackers%20used%20the%20%E2%80%9Cgrowth%20factor%E2%80%9D%20in%20the%20Memcached.

[189]ACSC Annual Cyber Threat Report 2020-21, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.

Endnotes

[190]Cyber Security Industry Advisory Committee, Locked Out: Tackling Australia's Ransomware Threat (March 2021), https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf.

[191]Cyber Security Industry Advisory Committee, Locked Out: Tackling Australia's Ransomware Threat (March 2021), https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf.

[192]Jaycee Roth, Data Exfiltration in Ransomware Attacks: Digital Forensics Primer for Lawyers (16 September 2021), https://www.kroll.com/en/insights/publications/cyber/data-exfiltration-ransomware-attacks.

[193]Cyber Cube, 'Understanding Criminal Cyber Threat Actors and Motivations', https://www.actuarialpost.co.uk/downloads/cat_1/CyberCube%202022%20Understanding%20criminal%20cyber%20threat%20actors%20and%20motivations.pdf.

[194]Allianz Global Corporate and Speciality, Ransomware trends Risks and Resilience (October 2021), https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html.

[195]Kurt Baker, Crowdstrike, Ransomware as a Service (RaaS) Explained (7 February 2022), https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

[196]Microsoft Defender Threat Intelligence, Ransomeware as a service: Understanding the cybercrime gig economy and how to protect yourself (9 May 2022), https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/.

[197]Microsoft Defender Threat Intelligence, Ransomeware as a service: Understanding the cybercrime gig economy and how to protect yourself (9 May 2022), https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/.

[198]Cyber Cube, 'Understanding Criminal Cyber Threat Actors and Motivations', https://www.actuarialpost.co.uk/downloads/cat_1/CyberCube%202022%20Understanding%20criminal%20cyber%20threat%20actors%20and%20motivations.pdf.

[199]Ireland Healthcare, Health Service Executive, faced a Conti ransomware attack in 2021, with the group reportedly demanding a $20 million ransom payment to decrypt files and data which included patient limiting the ability to preform numerous healthcare services: PWC, Conti cyber attack on the HSE: Independent Post Incident Review (3 December 2021) 6-9, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.

[200]FBI Flash Alert Number CP-000147-MW (20 May 2021), https://www.ic3.gov/Media/News/2021/210521.pdf.

[201]OWASP Top 10, https://owasp.org/www-project-top-ten/.

[202]US Government Accountability Office, Report to Congressional Requesters, Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach (August 2018) 10, https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf.

[203]Josh Fruhliner, Equifax data breach FAQ: what happened, who was affected, what was the impact? https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[204]ACSC Annual Cyber Threat Report 2020-21, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.

[205]ACSC, Cyber Supply Chain Risk Management, https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management.

[206]See, for example, International Committee of the Red Cross, Cyber-attack on ICRC: What we know, https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[207]Queensland Police, Boiler Rooms, https://www.police.qld.gov.au/safety-and-preventing-crime/r-u-in-control/boiler-rooms.

[208]AFP, Business Email Compromise cost Australian victims more than $79 million in the past year (10 July 2021), https://www.afp.gov.au/news-media/media-releases/business-email-compromise-cost-australian-victims-more-79-million-past.

[209]AFP, Business Email Compromise cost Australian victims more than $79 million in the past year (10 July 2021), https://www.afp.gov.au/news-media/media-releases/business-email-compromise-cost-australian-victims-more-79-million-past.

[210]ACSC Annual Cyber Threat Report 2020-21, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21.

[211]Jurita Lapientytė, Nigerian police busts prolific cybercrime syndicate (19 January 2022), https://cybernews.com/news/nigerian-police-busts-prolific-cybercrime-syndicate/.

[212]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[213]Kurt Baker, CrowdStrike, 'What is Cyber Espionage?' (1 June 2022), https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[214]Microsoft Threat Modeling Tool threats (25 August 2022), https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

[215]Tong Xin, and Ban Xiaofang, 'Online banking security analysis based on STRIDE Threat Model' (2014) 8.2 International Journal of Security and Its Applications 271-282.

[216]Tong Xin, and Ban Xiaofang, 'Online banking security analysis based on STRIDE Threat Model' (2014) 8.2 International Journal of Security and Its Applications 271-282.

[217]Microsoft Threat Modeling Tool (25 August 2022), https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool.

[218]Available at https://attack.mitre.org/.

[219]See MITRE Overview, https://collaborate.mitre.org/attackics/index.php/Overview.

[220]ENISA (European Union Agency for Cybersecurity), Octave, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html; W Sardjono and MI Cholik, 'Information systems risk analysis using octave allegro method based at deutsche bank' (2018) International Conference on Information Management and Technology (ICIMTech), IEEE 38-42.

[221]Christopher Alberts et al, 'Introduction to the OCTAVE Approach', Carnegie-Mellon University Software Engineering Institute (2003).

[222]BA Tucker, 'Advancing Risk Management Capability Using the OCTAVE FORTE Process', Carnegie Mellon University (2020).

[223]This comes from OWASP Threat Modeling Project, https://owasp.org/www-project-threat-model.

[224]OWASP Threat Model Cookbook, https://owasp.org/www-project-threat-model-cookbook/.

[225]OWASP Threat Dragon, https://owasp.org/www-project-threat-dragon/.

[226]OWASP Threat Modeling Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html.

[227]OWASP Ontology Driven Threat Modeling Framework, https://owasp.org/www-project-ontology-driven-threat-modeling-framework/.

[228]LINDDUN can be downloaded from https://www.linddun.org/downloads.

[229]Microsoft, Threat Modeling for drivers, https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers.

[230]It is available at https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf.

[231]Matt Rosenquist, Prioritizing Information Security Risks with Threat Agent Risk Assessment (December 2009, Intel).

[232]Michael Muckin and Scott C Fitch, A Threat-Driven Approach to Cyber Security (Lockheed Martin Corporation, 2019), https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf).

[233]Michael Muckin and Scott C Fitch, A Threat-Driven Approach to Cyber Security (Lockheed Martin Corporation, 2019), https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf).

[234]Rock Stevens et al, 'The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level' (Proceedings of the 27th USENIX Security Symposium, August 15-17, 2018, Baltimore, Maryland, USA0, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-stevens.pdf; Wenjun Xiong and Robert Lagerström Threat Modeling – A systematic literature review (2019) 84 Computers & Security 53-69, https://doi.org/10.1016/j.cose.2019.03.010; David B Fox, et al, Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions: Threat Model ATT and CK/CAPEC Version, MITRE (2018), https://www.mitre.org/sites/default/files/2021-11/prs-18-1725-ngci-enhanced-cyber-threat-model-for-financial-services-sector-institutions.pdf.

[235]This is available at https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/0-The_Web_Security_Testing_Framework.

FOR PUBLIC RELEASE