**<Insert country name>**

**NATIONAL CYBER RISK ASSESSMENT REPORT <Insert date>**

[Update contents page as you see fit]

1. Foreword
2. Acknowledgments
3. Executive Summary
4. Introduction
5. The NCRA Process
6. Data quality caveats
7. National Cyber Risk Posture

* Distribution of CII systems susceptible to cyber risk
* Threat Vectors in <insert country name>
* Threat Actors in <insert country name>
* Vulnerabilities in <insert country name>’s National CII
* Cyber governance posture
* Impact of Cyber Risk on the GDP of <insert country name>
* Impact of Cyber Risk on Critical Services

1. Cyber Risk Posture in Critical Sectors
   1. <Insert list of sectors e.g.
   2. Government
   3. Financial Services
   4. Energy
   5. Communications>

* Distribution of sector CII systems susceptible to cyber risk
* Threat vectors of concern to the sector
* Threat actors of concern to the sector
* CII vulnerabilities in the sector
* Impact of sector cyber risks on critical services

1. Recommendations
2. Appendices

* Appendix: List of Sectors and Stakeholders
* Appendix: List of Abbreviation

### **Foreword**

[For you to adjust as you see fit]

This document is a report of the National Cybersecurity Risk Assessment conducted and compiled by the <insert country name> <Insert name of department that has led the work>.

The objective of the exercises was to identify a national risk assessment framework of assets and resources in critical sectors and organisations that could be vulnerable to cyber security intrusion, attacks, hacking and destabilization.

The report is a record of the study, assessment and hands-on practical application of the cyber security workshop engagements in <insert country name>. It involved the use of critical methodologies, effort and resource to analyse critical national and resource risks.

This report shall be used to <insert how it will be used e.g. cyber strategy development, cyber risk reduction initiatives, etc.>

**Acknowledgements**

[For you to adjust as you see fit]

The leadership of the <Insert name of department that has led the work> wishes to express appreciation to the <insert names of organisations that have done the work> resilience and persistence in conducting the NCRA workshops in <insert country name>.

**Executive Summary**

[For you to adjust as you see fit]

<insert country name>’s National Cyber Authority, <Insert name of department that has led the work>, conducted <insert country name>’s <first> NCRA survey questionnaire between <insert start date> and <insert end date>. Over <Insert number of organisations> organisations from across <insert number of sectors> sectors participated in the survey and identified <insert number of identified systems> systems, which they rated for cyber risk.

The quality of the survey response data was <good / ok>, and suitable for analysis. The data has enabled the generation of both national and sector views of cyber risk, cyber threat, impact and vulnerability.

Each system was assessed for risk based on likelihood and impact. And the initial analysis has identified <insert number of systems in highest zone> of the <insert number of systems identified> CII systems in the highest risk zone, with a further <insert number of systems in orange zone> systems in the next highest risk category. This <updates / forms> <insert country name>’s <first prioritised> cyber risk asset register.

The most critical systems are in the <insert names of top 2 sectors> sectors, with <insert number of sectors> sector having systems in the high-risk zone. The national cyber authority and appropriate CII organisations need to check the ratings for each of the systems, understand them better, and ideally identify and take actions to reduce their risk levels.

As a national level threat summary, <insert name of main threat actor> using <insert name of main threat vector> are the biggest cyber threats, with < insert number of> vectors and actors being deemed of very high concern. At a sector level there were some differences, with <insert names of specific actor and vectors> being more relevant to some sectors than others.

Most cyber vulnerabilities appear to be in the <insert name(s) of highest rated sector(s)> sectors, with the <insert name of least rated sector> sector having the least. [Include if true: Overall, vulnerability ratings look a little on the low side, possibly because few organisations like to admit to weaknesses, and/or have a distrust of how that information will be used. Note that an increased level of openness is needed to ensure the best possible insights.]

At over <include percentage>% GDP, the <insert name of highest GDP impact sector> sector has the biggest potential total worst-case impact of $<include $ number>M, with the <insert name of next highest sector> sector reporting a potential $<include $ number>M impact.

Overall, this is a very useful NCRA for <insert country name> and should lead to actions that will set <insert country name> on a more focused path towards stronger national cyber security.

**Introduction**

[For you to adjust as you see fit]

This report is the result of <insert country name>’s Government surveying the owners of Critical National Infrastructure (CNI), to deliver an initial picture of cyber security risk to Critical Information Infrastructure (CII). The report presents the results of the analysis of the data provided by each participating organisation in their responses to a questionnaire sent out by <insert name of organisation leading the NCRA>. The survey questionnaire captures the characteristics of each system that delivers a critical service. And the results for each system are aggregated together to form a sector wide and national risk picture.

The analysis in this report covers the national picture and sector views for the <Insert names of all sectors that provided information> sectors. However, the overall objective applies to other sectorial institutions pertinent to national Cyber Security.

No organisations or systems are named in this report, with the information being entirely anonymous.

**The NCRA Process**

A National Cyber Risk Assessment (NCRA) consists of an interactive self-assessment questionnaire, with the capture of cyber-security risk through workshop-based activity and analysis. It has been developed from international and UK best practice; using risk and cyber ISO standards, and national guidance for defending people and businesses against cyber-attacks. It is a repeatable process that is tailored to the needs of each country.

The NCRA is relevant for national cyber security authorities who can use it to inform their national cyber security strategy. For sector authorities who can use it to provide strategic assessments of cyber defence readiness. And for individual organisations who can use it to provide insight on their risks to operations.

The NCRA measures and analyses the national level of cyber risk. The findings are usually delivered through a formal report that details risk impacts & likelihoods and an assessment of national capability maturity. A set of recommended risk mitigations are included based on the risks identified. These are tailored towards those organisations with high risk systems that would incur the highest national impact. Advice is also provided on how to deliver those risk mitigations. Therefore, the NCRA helps a country to prioritise its limited resources to build cyber defence capacity and capability.

The NCRA is done through a local National Authority for cybersecurity, with the first iteration often done with limited assistance from a UK team. The National Authority identifies the essential stakeholders and scopes the assessment process to meet national requirements. The UK team helps the National Authority with planning the first iteration, and access to the NCRA portal that contains guidance, tools and training.

There are four stages to a NCRA, these are: ‘Identification’ to agree the scope and senior sponsor; ‘Initiation’, to communicate the purpose to all stakeholders; ‘Implementation’, to conduct survey and analysis; and finally, ‘Next steps’ where conclusions and actions are agreed.

**Data quality caveats**

This is the <insert first / second / other> time that <insert country name> has run a NCRA. Many CII organisations have provided useful, comprehensive and realistic data. However, some have chosen not to respond, and others have provided data that have gaps and discrepancies. If <insert country name>’s cyber champions are going to take substantial action based on this NCRA e.g. create a realistic and appropriate cyber strategy, they must have high confidence in the quality of the underlying data.

A screenshot of a cell phone

Description automatically generatedThe NCRA analytic spreadsheet, into which all questionnaire responses are collated, has basic built-in tests to assess data quality. These tests identify gaps, repeated information, and areas where the responses may be at the wrong end of the questionnaire spectrum. As you can see from this example (not related to this report), there can be sometimes be room for data quality improvements.

The need for improved data quality is always to be expected. It takes time and repeated cyber risk assessments for representatives of CII organisation to improve their cyber assessment maturity and gain confidence in how the data is going to be stored, processed and used.

Until everyone provides great quality data careful consideration of the processed results is needed. And this should be borne in mind at all times when reviewing, drawing conclusions and identifying actions.

This report highlights where some revision of answers would be advisable.

**National Cyber Risk Posture**

[For you to adjust as you see fit]

The following pages provide the <insert first / second / other > national cyber risk picture of <insert country name>’s exposure to cyber risk. And provide an opportunity for the National Authority and the contributing CII organisations to discuss and take action on the <preliminary> findings.

Overall, there are a lot of useful insights and recommendations that can be extracted from the graphs and charts (see list of recommendations at the end of this report).

However, there is room for improvement, especially around some aspects of data quality, where for instance a re-calibration / normalisation of <state an area where this is advisable> would be a sensible activity. Therefore, some results should be investigated further rather than accepted just at face value.

Distribution of CII systems suspectable to cyber risk

The Probability – Impact Grid is one of the most important outputs from the NCRA, as it highlights the overall criticality of <insert country name>’s CII systems. As can be seen, the grid contains <insert number of> identified CII systems in a widespread from low risk to high risk.

[include picture of national probability – impact grid from analytic spreadsheet]

Most importantly there are <insert number of high-risk systems> CII systems that are in the high risk ‘red’ zone. <insert names of sectors> sectors have systems in the high-risk zone. Ideally all of these systems should be reviewed, along with those in the orange zone just to make sure that they are not really in the red zone too. [Include of true: Note that this picture is typical of what would be expected for a national level view of critical systems.]

A detailed focus on addressing risk for all these systems in all sectors may be too much for <insert country name> to achieve in a short time period. Therefore, a more detailed analysis should be done to understand the specific risks to these systems, and which ones should be prioritised for remediation. This could be done in concert with the findings from vulnerabilities, impacts, and existing national cyber improvement objectives, to create a short list of systems where the cyber risk should be reduced.

Threat Vectors in <insert country name>

The NCRA allows respondents to focus on the most critical cyber threat vectors. For <insert country name>, the greatest perceived threat vectors are <insert name of top vector threat> and <insert name of second top vector threat>, which <insert number of sectors> sectors reported in their ‘top two’.

[include picture of national threat vectors from analytic spreadsheet]

<include any comments on aspects that are surprising e.g. levels similar, unusual suspects rated highly, usual suspects rated lowly, etc.>

It would be useful to investigate whether CII organisations in <insert country name> are being attacked via these threat vectors and how many attacks are actually occurring.

Threat Actors in <insert country name>

The NCRA focuses on the most common cyber threat actors. As can be seen, the greatest threat actor is the <state highest threat actor>. It is therefore apparent that this is an actor type that <insert country name> needs to be taking significant action to guard against. In some sectors such as <insert name of another sector that a different threat actor is a concern>, it is <insert name of relevant threat actor> that is the main issue, while <insert name of other sector(s) that a different threat actor is a concern> also worry a lot about <insert name of relevant threat actor>.

[include picture of national threat actors from analytic spreadsheet]

<include any comments on aspects that are surprising e.g. levels similar, unusual suspects rated highly, usual suspects rated lowly, etc>

Vulnerabilities in <insert country name>’s National CII

The vulnerabilities are based on the UK’s National Cyber Security Centre’s ’10 Steps to Cyber Security’. Without having good defences in place to reduce vulnerabilities assets are exposed to attacks.

At first glance, the data provided appears to show that CII owning organisations in <insert country name> largely see <few / some / many> major vulnerabilities in their assets, with <only a little / a lot of> ‘red’.

Assuming respondents have been a little coy about admitting vulnerabilities then using the information in all but green zones it is <insert names of top 3 greatest vulnerabilities> are the areas of greatest vulnerability. And <insert country name> should focus on rectifying these.

[include picture of national vulnerabilities from analytic spreadsheet]

Cyber governance posture

Cyber governance has become a hot topic worldwide, with boards of organisations held to account for ensuring that, from the ‘top down’, cyber security is being managed. [Only include if true: As many banks and telcos are international and have strong cyber security approaches, it is not surprising to see that cyber governance is either OK or very good across those organisations.]

The graphic below shows the prominence of cyber security across the <insert names of sectors> sectors. It is clear, that as a minimum, there is a requirement to look at future initiatives to help these sectors to reinforce cyber security governance. Improvements should be focused at the board level and downwards to ensure that cyber training, cyber risk registers, cyber roles and responsibilities, etc. are in place and being properly executed. However, as this is such an important area to get right it would probably benefit <insert country name> if all those organisations in the OK zone received a boost or focused on this.

[include picture of national cyber governance from analytic spreadsheet]

Impact of Cyber Risk on the GDP of <insert country name>

The finances of any country are hugely important to its continued prosperity and functioning operations. Cyber-attacks can have a huge impact on the direct and indirect cash reserves and the longer-term ability for a country to acquire and service debts. The NCRA questionnaire asks organisations to determine GDP impact based on their realistic worst-case scenario for that system. The GDP impact analytic assumes that ALL worse case scenarios happen simultaneously, so the results may be exaggerated but very often dependencies are not well understood so chain-reaction impacts could occur. Please treat this as a guide rather than an absolute.

The GDP of <insert country name> is around $<insert country‘s GDP>M. The greatest cyber system impacts to GDP would happen from the <insert name of highest GDP impact sector> sector with a $<insert amount>M impact and <insert name of 2nd highest GDP impact sector> sector with a $<insert amount>M.

Overall, it is likely that <insert country name> is exposed to somewhere between <insert low percentage>% and <insert high percentage>% of its GDP if a significant cyber-attack affected many organisations for a sustained period.

Impact of Cyber Risk on Critical Services

Impacts are not just limited to money, with critical services affected from cyber-attacks in other sectors. Although the <insert names of main sectors> sectors would be severely impacted, cyber-attack impacts in <insert country name> would affect many other sectors, with <insert names of main ‘knock on’ sectors> all taking significant hits.

[include picture of impact to critical sectors / services, from analytic spreadsheet]

It is recommended that <insert country name> investigate the dependencies between the various systems in each sector to understand how a cyber-attack would propagate and disrupt these other sectors’ systems. A follow-on exercise should then be conducted to understand how those impacts could be mitigated.

Use of threat intelligence

Cyber attackers often appear to have an advantage as they attack globally and often indiscriminately, gaining access to systems, money and data. However, the advantage is largely with the defender and owner of the CII, and the use of threat intelligence is one method to take back control.

There are many sources of threat intelligence from open source, community sharing to commercial offerings; with low to high frequency updates; and low to high quality information available.

The organisations in <insert country name> all appear to <comment on regard of> threat intelligence. However, it appears that <comment on which sectors have TI use below that needed> sectors are using threat intelligence below the level needed to properly understand and mitigate their cyber threats; with <insert names of biggest gap sector> organisations at a distinct disadvantage.

[include picture of use of threat intelligence, from analytic spreadsheet]

<include any final comments on threat intel e.g. warnings, revisits to data, etc.>

**[Repeat this section (2 pages) for each sector]**

**[Include charts / graphs about sectors in analytic spreadsheet]**

**[For neatness, word-wrap the text around the scaled pictures]**

**Cyber Risk Posture in Critical Sectors: <Insert sector name> Sector**

These are the analysed results and comments related to the <insert sector name> Sector CII organisations. Overall there are <insert number of system in sector> <insert sector name Sector> CII systems in the high-risk zone, that <insert name of greatest threat actor for this sector> could attack using <insert name of greatest threat vector for this sector>, through a range if vulnerabilities including weaknesses in <insert name of worst vulnerability for this sector>. The impacts are quite significant with a GDP impact of $<insert GDP impact value for this sector>M and disruption to other <insert names of top 3 impacted sectors>.

Distribution of <insert sector name> sector CII systems susceptible to cyber risk

[include picture of sector’s probability – impact grid from analytic spreadsheet]

The <insert sector name> sector has quite a wide range of systems, with <comment on system risk distribution>. These should be further investigated to understand their importance and real-world impacts from a cyber-attack.

Threat vectors of concern to the <insert sector name> sector

[include picture of sector’s threat vectors from analytic spreadsheet]

The greatest cyber threat vectors to <insert sector name> sector CII systems are <insert name of sector’s highest threat vectors>.

These should be investigated further with analysis of roles, processes, info and tools that could be used to reduce the threat from these vectors.

Threat actors of concern to the <insert sector name> sector

[include picture of sector’s threat actors from analytic spreadsheet]

By far the greatest cyber threat actor to <insert sector name> sector CII systems is <insert name of sector’s highest threat actor>, with <insert name sector’s next highest threat actors> a slightly lesser concern.

The <insert sector name> sector’s organisations should review the susceptibility of their systems to <insert name of sector’s highest threat actor> and determine how to detect and deter.

CII vulnerabilities in the <insert sector name> sector

[include picture of sector’s vulnerabilities from analytic spreadsheet]

The <insert sector name> sector appears exposed to exploits in <insert names of top 3 worst vulnerabilities>.

<insert sector name> sector organisations should work on closing these weaknesses first, and then <list next set of worst vulnerabilities for this sector>.

Impact of <insert sector name> sector cyber risks on critical services

[include picture of knock on sectors and services from analytic spreadsheet]

The impacts from <insert sector name> sector systems to other sectors are <insert level of significance> with disruption to a <insert range> of systems in other sectors.

It would be useful for <insert sector name> sector organisations to understand their dependencies with systems in other <insert names of dependent services / sectors>. And then work out how follow-on impacts could be minimised.

**Recommendations**

[For you to adjust as you see fit]

This section draws together the various recommendations in the report that should be considered as immediate actions. Each recommendation clearly articulates whether it is for CII organisations, a CII sector, the National Authority, or some joint activity.

[These are a template set. Only keep if true. Use data to identify others]

Recommendation 1: Engage directly with CII organisations to help them understand their cyber security risk. And where necessary improve the quality of the survey data e.g. by providing more discerning and effective responses to NCRA questions. Until this is done, results should be interpreted with care and not just at face value.

Recommendation 2: CII organisations to check the ratings for each of the systems, understand them better, and ideally identify and take actions to reduce their risk levels. This applies to all in the red (highest) and orange (second highest) risk zones. This could be done in concert with the findings from vulnerabilities, impacts, and existing national cyber improvement objectives, to create a short list of systems where the cyber risk must be reduced immediately. It is recommended that the <insert name of organisation leading the NCRA> works in partnership with those organisations owning the most critical systems to help develop minimum standards for enhanced cyber security.

Recommendation 3: CII organisations to do more individual organisation analysis to understand how each actor type is going to attack their CII systems. This should include enhanced use of threat intelligence and cyber-attack simulations/exercises.

Recommendation 4: CII organisations to reduce specific vulnerabilities. A standard package of advice and guidance based on the 10 steps to cyber security, system audit/testing and adopting minimum cyber security standards should all be considered.

Recommendation 5: Help specific organisations from the board level downwards improve their cyber governance e.g. ensure that cyber training, cyber risk registers, cyber roles and responsibilities, etc. are in place and being properly executed.

Recommendation 6: CII organisations to investigate the dependencies between the various systems in each sector, to understand how a cyber-attack would propagate and disrupt other sectors’ systems. Then understand how much impact this causes and how it can be reduced.

Recommendation 7: Consider developing a nationally led programme of testing and exercising beginning with the most critical system.

Recommendation 8: Revisit the national picture on cyber skills, awareness and training to assess the validity of the optimistic picture given by this initial survey.

Recommendation 9: <insert name of organisation leading the NCRA> to work with <insert names of sectors with biggest gap in threat intel use> to improve their access to, and use of, relevant threat intelligence.

**Appendix: List of Sectors and Stakeholders**

[For you to adjust and change rows as you see fit]

|  |  |  |
| --- | --- | --- |
| **No** | **Organisation** | **Abbreviation** |
| 1 | e.g. Ministry of <insert ministry name> |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| 8 |  |  |
| 9 |  |  |
| 10 |  |  |
| 11 |  |  |
| 12 |  |  |
| 13 |  |  |
| 14 |  |  |
| 15 |  |  |
| 16 |  |  |
| 17 |  |  |
| 18 |  |  |
| 19 |  |  |
| 20 |  |  |
| 21 |  |  |
| 22 |  |  |
| 23 |  |  |
| 24 |  |  |
| 25 |  |  |
| 26 |  |  |
| 27 |  |  |
| 28 |  |  |
| 29 |  |  |
| 30 |  |  |

**Appendix: List of Abbreviations**

[For you to adjust as you see fit]

CII: Critical Information Infrastructure

CNI: Critical National Infrastructure

GDP: Gross Domestic Product (aka revenue of a country)

NCRA: National Cyber Risk Assessment