



ZICTA

National Cyber Risk Assessment Report



www.zicta.zm

Contributors

This report has been developed by the Zambia Information and Communication Technology Authority (ZICTA), including key stakeholder entities and their respective resource personnel who cannot be mentioned for security and confidentiality reasons.



Design & Layout by: Paul Sinyinda, Images by iStockPhoto.com

Copyright © 2021 By the Zambia Information and Communications Technology Authority (ZICTA)
Stand No. 4909, Corner of Independence and United Nations Avenues, P.O. Box 36871, Lusaka, Zambia

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without prior permission.



National Cyber Risk Assessment Report

September 2022

Contents

Contents.....	5
Foreword	6
Acknowledgements	7
Executive Summary	8
1. Introduction	9
2. The NCRA Process.....	10
3. Data Quality Caveats	11
4. National Cyber Risk Posture.....	12
5. Cyber Risk Posture in Critical Sectors: Private (Organisation) Sector	19
6. Cyber Risk Posture in Critical Sectors: Aviation Sector.....	22
7. Cyber Risk Posture in Critical Sectors: Banking & Finance Sector.....	25
8. Cyber Risk Posture in Critical Sectors: Energy Sector	27
9. Cyber Risk Posture in Critical Sectors: Government Sector	29
10. Cyber Risk Posture in Critical Sectors: Healthcare Sector	31
12. Cyber Risk Posture in Critical Sectors:	36
Land and Transport Sector	36
13. Cyber Risk Posture in Critical Sectors: Water Sector	38
14. Cyber Risk Posture in Critical Sectors: Water Sector	40
Recommendations.....	42
Appendices	44

Foreword

This document is a report of the National Cybersecurity Risk Assessment conducted and compiled by the Zambia Information and Communication Technology Authority (ZICTA).

The objective of the exercise 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 destabilisation.

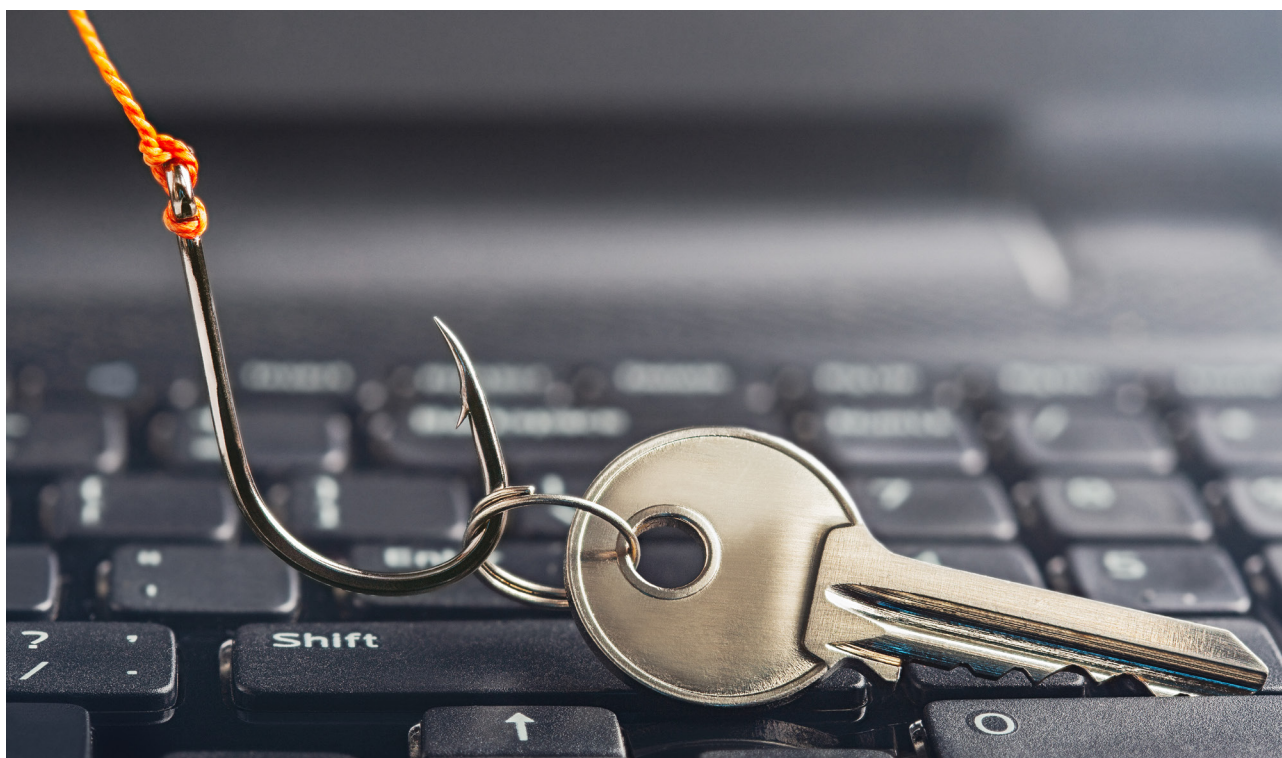
This report is a record of the study, assessment and hands-on practical application of the cyber security workshop engagements for the exercise. It involved the use of critical methodologies, effort and resource to analyse critical national and resource risks.

This report shall be used to drive cyber risk reduction initiatives and cyber strategy development.

Acknowledgements

ZICTA wishes to express appreciation to the UK Home Office for their support, resilience and persistence in supporting the NCRA exercise in Zambia. ZICTA also wishes to express appreciation to the institutions that participated in the National Cyber Risk Assessment Process.

Executive Summary



ZICTA conducted Zambia's first NCRA survey questionnaire between January 18, 2022 and March 20, 2022. Organisations from across 10 sectors participated in the survey and identified 200 systems, which they rated for cyber risk.

The quality of the survey response data was good, 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 32 of the 200 CII systems in the highest risk zone, with a further 37 systems in the next highest risk category. This forms Zambia's first cyber risk asset register.

The most critical systems are in the Information & Communication, Banking & Finance and Healthcare sectors, with 5 sectors having systems in the high-risk zone. ZICTA 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, Cyber Criminals using Malware are the perceived biggest cyber threats, with 4 threat vectors and actors being deemed of very high concern. At a sector level there were some differences, with Accidents and Phishing being perceived to be more relevant to some sectors than others.

The highest level of cyber vulnerabilities appear to be in the Government, Healthcare and Water sectors, with the Organisation (Private) sector having the least. 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 3% GDP, the Banking and Finance sector has the biggest potential total worst-case impact of \$2,351,244,000, with the Government sector reporting a potential \$1,903,020,000 impact.

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

1. Introduction



This report is the result of Zambia Information and Communication Technology Authority (ZICTA) surveying the owners of Critical Information Infrastructure (CII), 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 ZICTA. 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 sector wide and national risk pictures.

The analysis in this report covers the national picture and sector views for the Organisation (Private Sector), Aviation, Banking & Finance, Energy, Government, Healthcare, Information & Communication, Land Transport, Water and Education 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. This is to ensure organisation anonymity and encourage continued participation without fear of persecution.

2. The NCRA Process

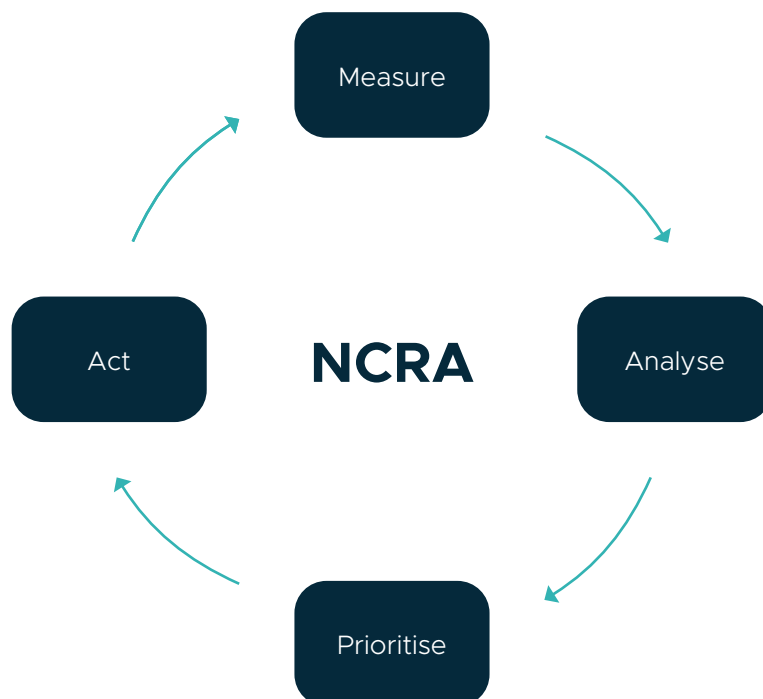
A National Cyber Risk Assessment (NCRA) consists of an interactive self-assessment questionnaire, with the capture of cyber-security risk through workshop-based activity and analysis. It has been developed from international and UK best practice; using risk and cyber ISO standards, and national guidance 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 Authority with planning the first iteration, and access to the NCRA portal that contains guidance, tools and training. No raw (non-anonymised) data is shared with the UK team, all data remains in Zambia and is only accessed by authorised persons such as relevant Authority personnel.

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.



3. Data Quality Caveats

This is the first time that ZICTA 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 Zambia’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.

The 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 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.

-2 Data Gaps	-2 Data Gaps	-2 Data Gaps	-2 Data Gaps	-2 Data Gaps
	Check CIA	Check CIA	Check CIA	Check CIA
	Same Actor scores	Same Actor scores		
	Same Actor scores	Same Actor scores	Similar Vector scores	Similar Vector scores
Same Vulnerability scores	Same Vulnerability scores	Same Vulnerability scores		
				High Vulnerability average

4. National Cyber Risk Posture

The following pages provide the first national cyber risk picture of Zambia's exposure to cyber risk. And provides an opportunity for ZICTA 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 impacts to CII systems would be a sensible activity. Therefore, some results should be investigated further rather than accepted just at face value.

4.1. Distribution of CII Systems Susceptible to Cyber Risk

The Probability – Impact Grid is one of the most important outputs from the NCRA, as it highlights the overall criticality of Zambia's CII systems. As can be seen, the grid contains 200 identified CII systems in a widespread from low risk to high risk.

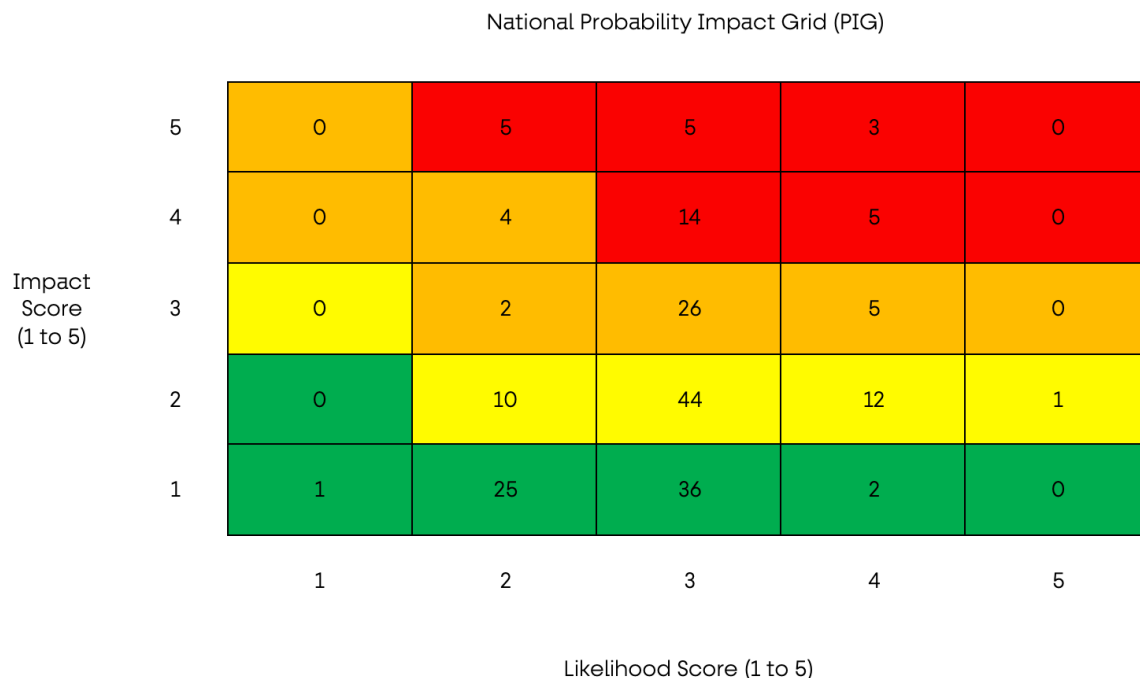


Figure 3: National probability – impact grid

Most importantly there are 32 CII systems that are in the high risk 'red' zone. 5 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. Furthermore, the systems identified in yellow and green zones have a smaller national level impact but are still of great importance to the organisations operating them. 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 Zambia 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.

4.2. Threat Vectors in Zambia

The NCRA allows respondents to focus on the most critical cyber threat vectors. For Zambia, the greatest perceived threat vectors are Malware and Phishing, which 6 sectors reported in their 'top two'.

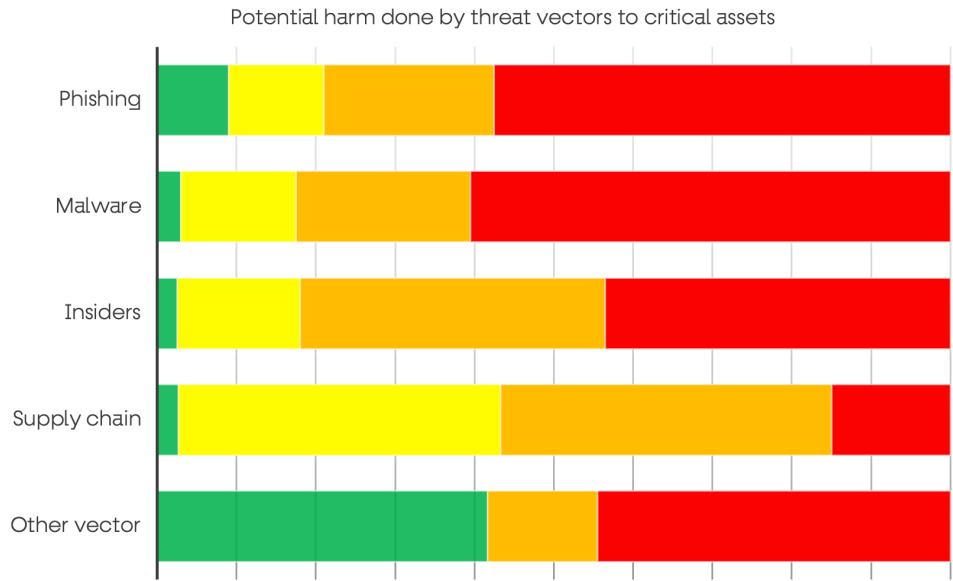


Figure 4: National Threat Vectors

While it was expected to have Malware in among the highly rated threat vectors, it is interesting to see how highly rated Phishing is as a threat vector across multiple sectors and organisations. It would be useful to investigate whether CII organisations in Zambia are being attacked via these threat vectors and how many attacks are actually occurring.

4.3. Threat Actors in Zambia

The NCRA focuses on the most common cyber threat actors. As can be seen, the greatest threat actor is the cyber criminals. It is therefore apparent that this is an actor type that Zambia needs to be taking significant action to guard against. In some sectors such as Education, it is Accidents that is the main issue.

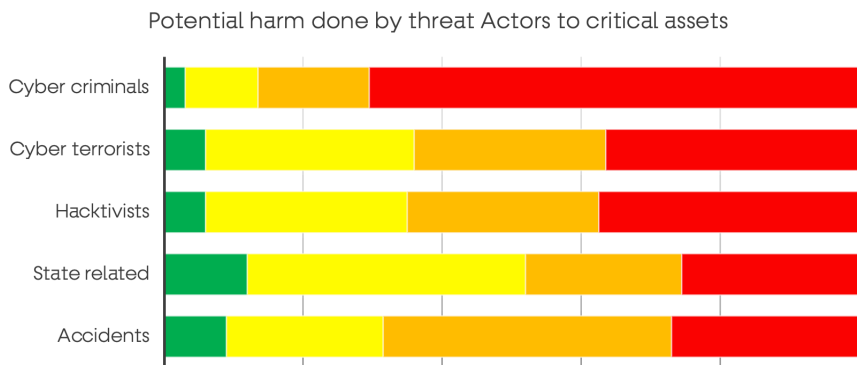


Figure 5: National Threat Actors

While it was expected to have Cyber Criminals among the highly rated threat actors, It is interesting to see how highly rated Accidents is as a threat actor in some sectors and organisations.

4.4. Vulnerabilities in Zambia’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 Zambia largely see few major vulnerabilities in their assets. The red and orange present indicates some major weaknesses in controls being used, and this is of great concern to CII related systems that need to meet a high bar when it comes to vu.

Assuming respondents have been a little coy about admitting vulnerabilities then using the information in all but green zones, it is user education, malware prevention and network security that are the areas of greatest vulnerability. And Zambia should focus on rectifying these.

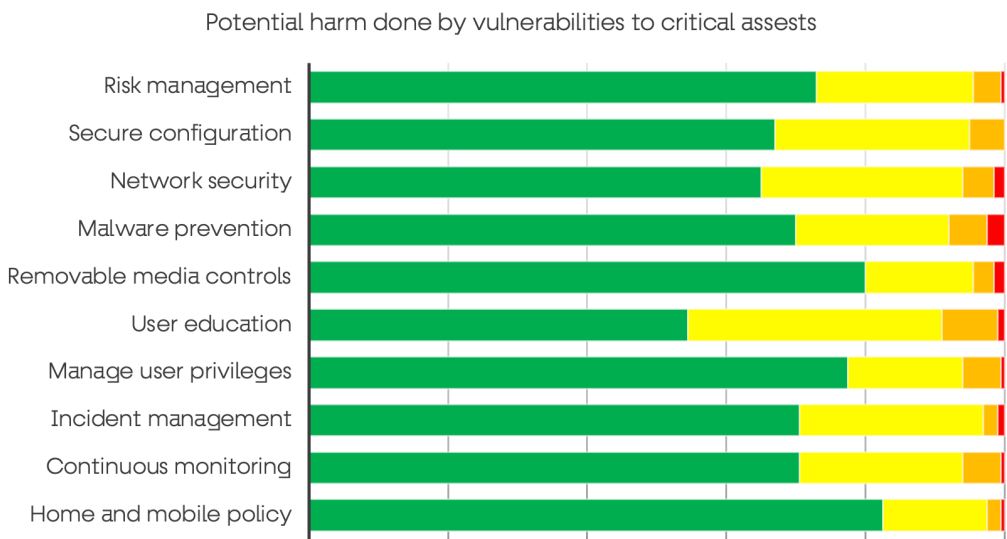


Figure 6: National Vulnerabilities

4.5. 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. 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 graphics below show the prominence and responsibilities of cyber security across the Organisation (Private Sector), Aviation, Banking & Finance, Energy, Government, Healthcare, Information & Commu- nication, Land Transport, Water, Food and Education 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 Zambia if all the organ- isations in the OK zone received a boost or focused on this, and all the organisations ‘no’ zone received guidance on how to assign responsibility for systems.

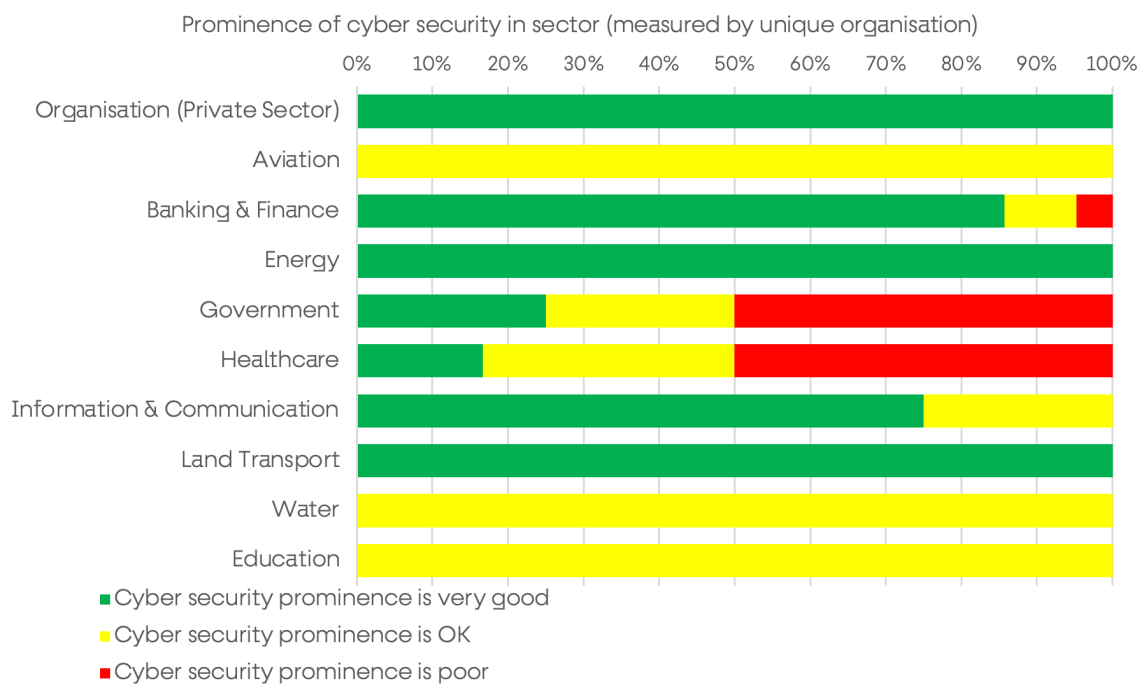


Figure 7: National Cyber Governance – Cyber Security Prominence

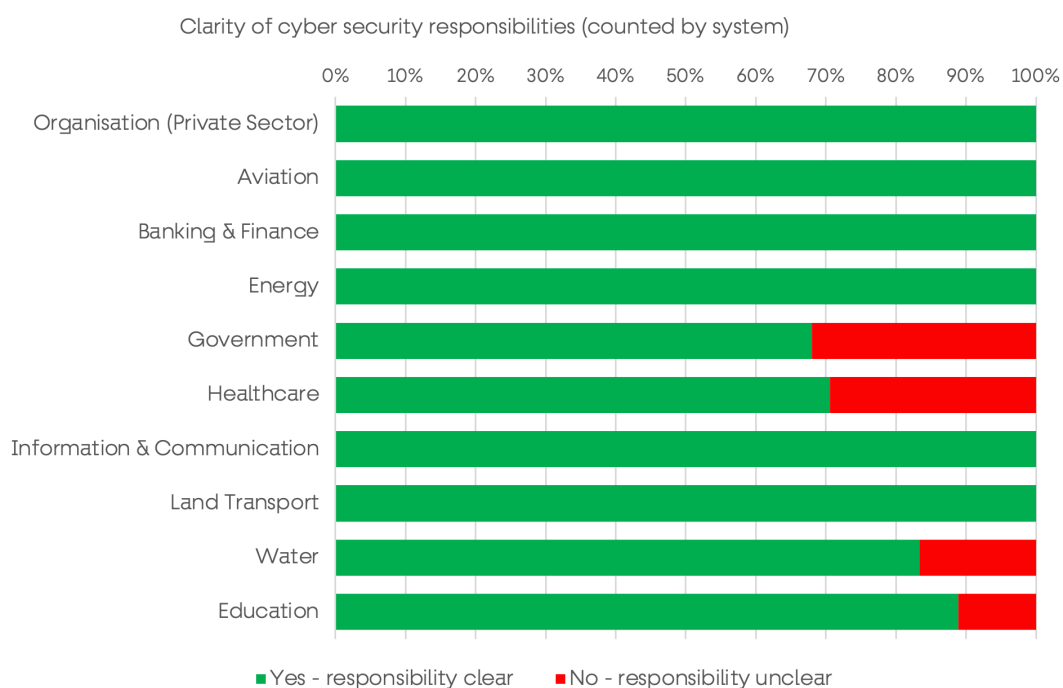


Figure 8: National Cyber Governance – Cyber Security Responsibilities

4.6. Impact of Cyber Risk on the GDP Of Zambia

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.

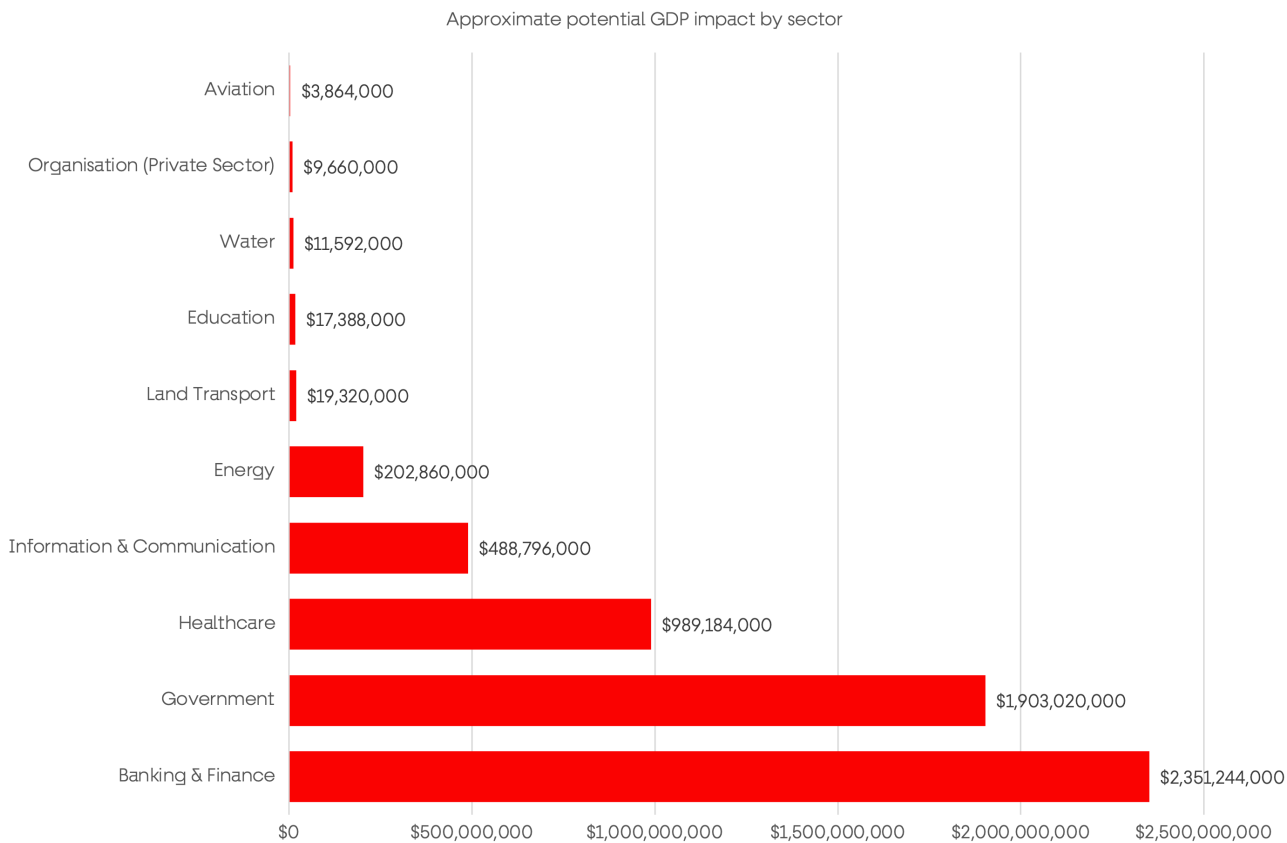


Figure 9: National GDP Impact by Sector

The GDP of Zambia is around \$19,320,000,000. The greatest cyber system impacts to GDP would happen from the Banking & Finance sector with a \$2,351,244,000 impact and Government sector with a \$1,903,020,000.

Overall, it is likely that Zambia is exposed to somewhere between 0.01% and 12.17% of its GDP if a significant cyber-attack affected many organisations for a sustained period.

4.7. 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 Banking & Finance, Private (Organisation) and Government sectors would be severely impacted, cyber-attack impacts in Zambia would affect many other sectors, with Healthcare, Information & Communication and energy to mention a few all taking significant hits.

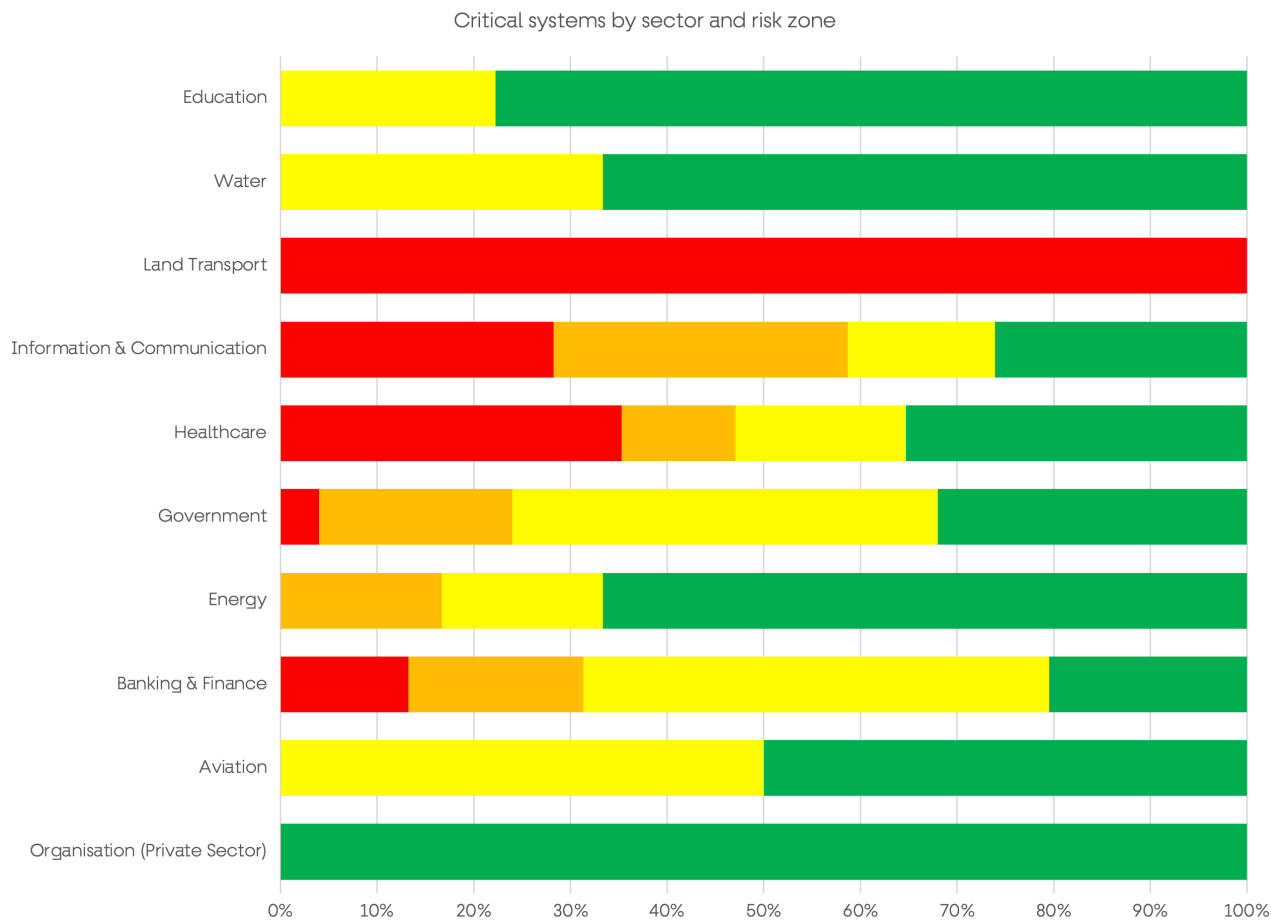


Figure 10: Impact to Critical Sectors / Services

It is recommended that Zambia 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.

4.8. 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 Zambia appear to have a medium to high perception of threat intelligence importance, and do not perceive such information to be of critical value. Moreover, based on the submissions, some organisations do adequately make consultation with experts on threat intelligence. However, it appears that most organisations in the Education, Land Transport, Aviation and Healthcare sectors are using threat intelligence below the level needed to properly understand and mitigate their cyber threats; with Land & Transport organisations at a distinct disadvantage.

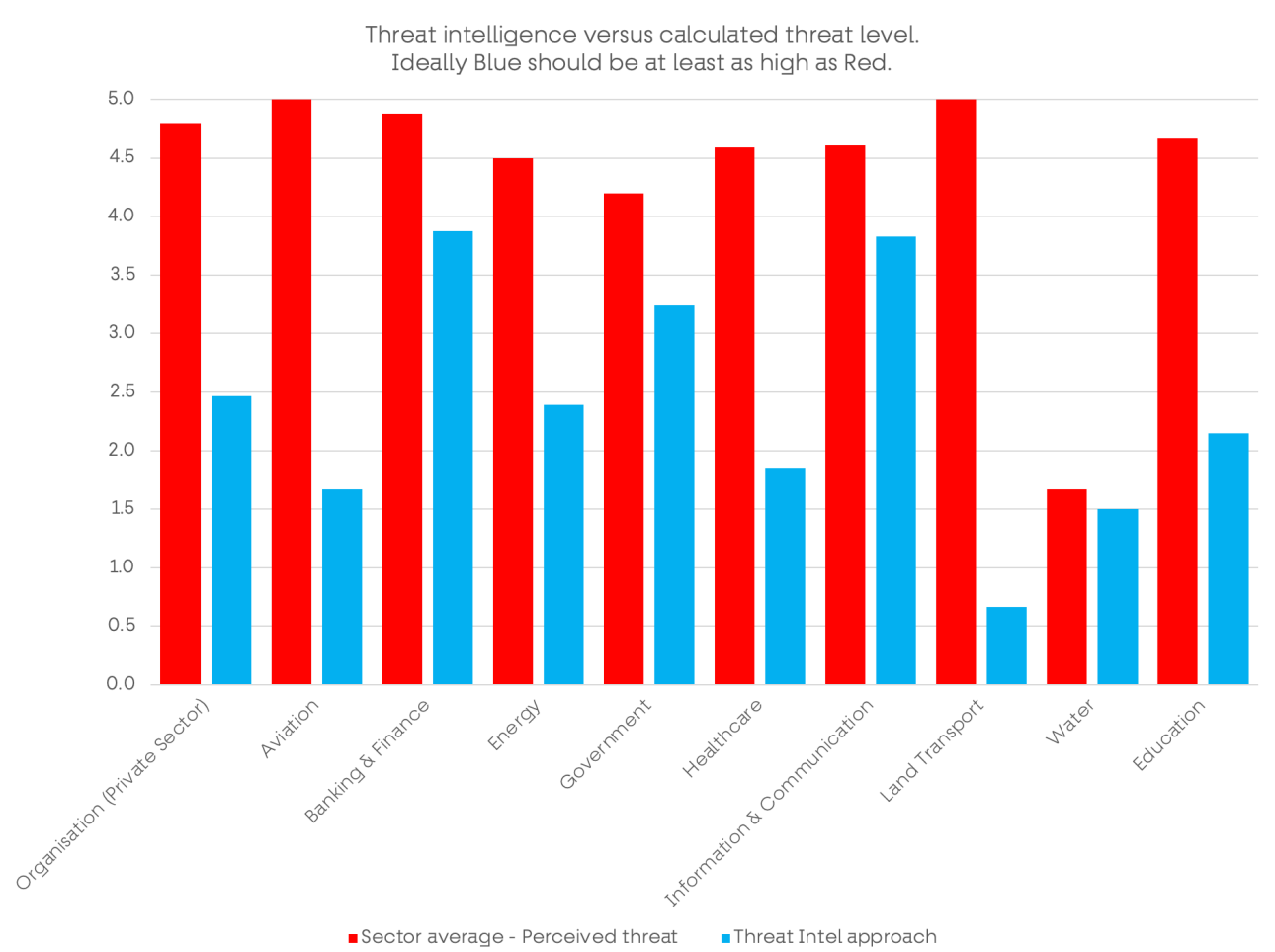


Figure 11: Threat Intelligence Versus Calculated Threat Level—Ideally blue should be at least as high as red

The Private (Organisation), Aviation, Energy, Healthcare, Land & Transport and Education sectors are in the severe danger zone and will remain there if they do not make significantly better use of various threat intelligence approaches immediately. The Banking & Finance sector is in the danger zone, while the Government, Water and Information & Communication sectors are in the warning zone and should consider additional threat intelligence usage.

5. Cyber Risk Posture in Critical Sectors: Private (Organisation) Sector

These are the analysed results and comments related to the Private (Organisation) Sector CII organisations. Overall there are no Private (Organisation) Sector CII systems in the high-risk zone, that cyber criminals could attack using phishing, through a range of vulnerabilities including weaknesses in user education. The impacts are minimal with a GDP impact of \$9,660,000 and disruption to other organisations in the Banking & Finance sector.

5.1. Threat Vectors of Concern to the Private (Organisation) Sector

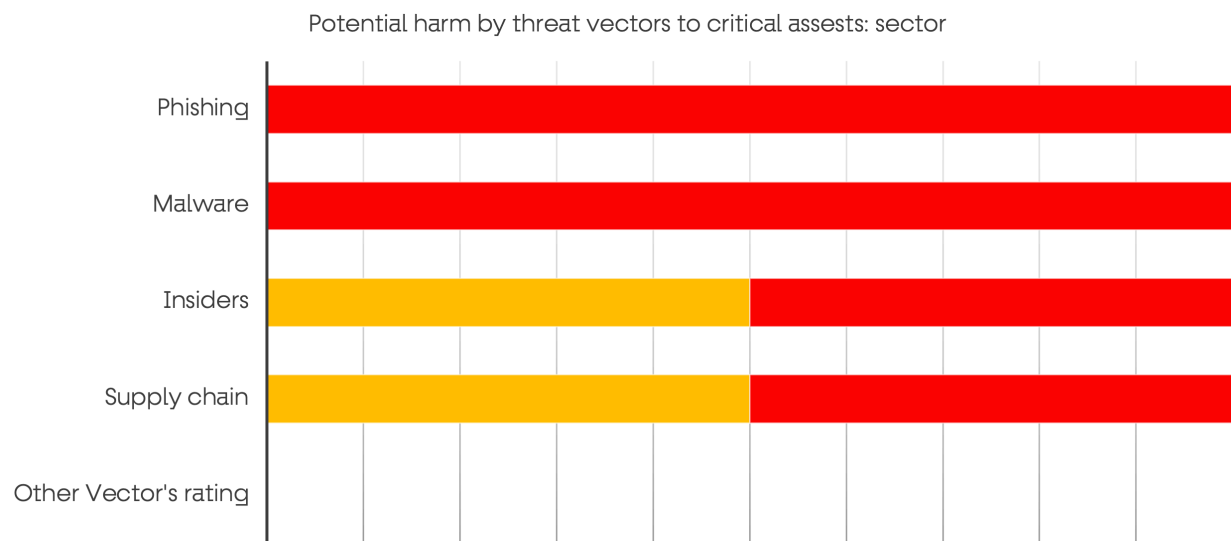


Figure 13: Private (Organisation) Sector's Threat Vectors

The greatest cyber threat vectors to Private (Organisation) Sector CII systems are phishing and malware.

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

5.2. Threat Actors of Concern to the Private (Organisation) Sector

The greatest cyber threat vectors to Private (Organisation) Sector CII systems are phishing and malware.

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

5.2. Threat Actors of Concern to the Private (Organisation) Sector

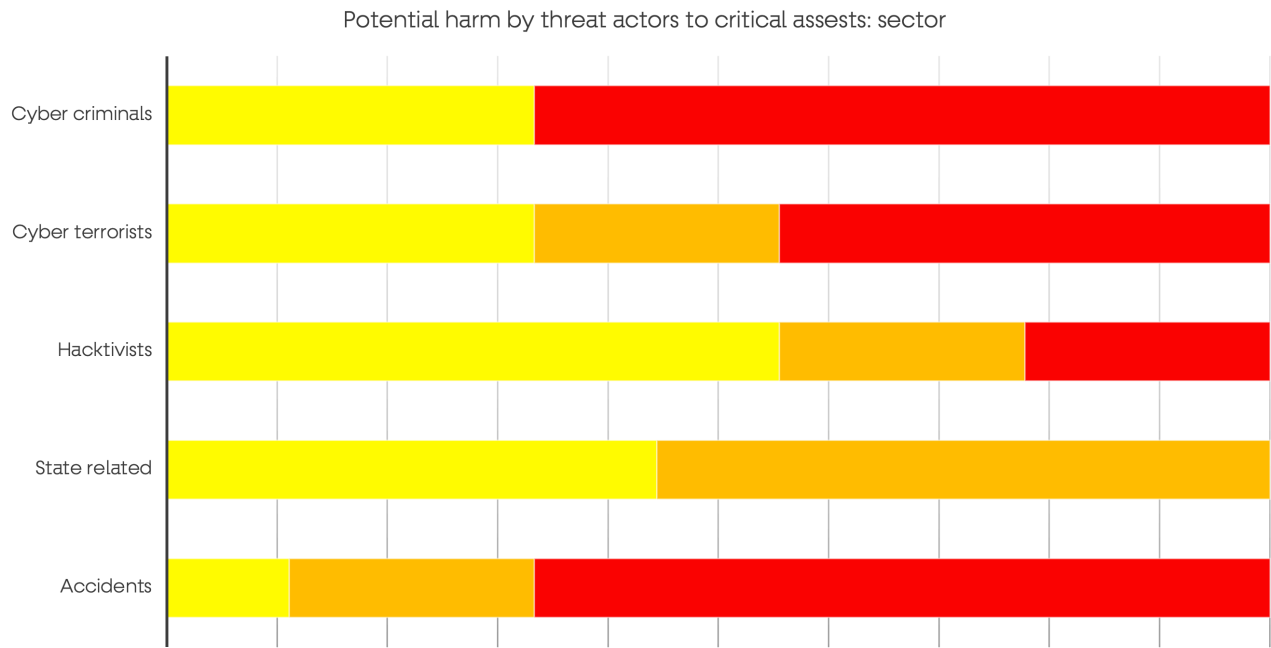


Figure 14: Private (Organisation) Sector's Threat Actors

By far the greatest cyber threat actor to Private (Organisation) Sector CII systems is Cyber Criminals, with Accidents a slightly lesser concern.

The Private (Organisation) Sector's organisations should review the susceptibility of their systems to Cyber Criminals and determine how to detect and deter.

5.2. CII Vulnerabilities in the Private (Organisation) Sector

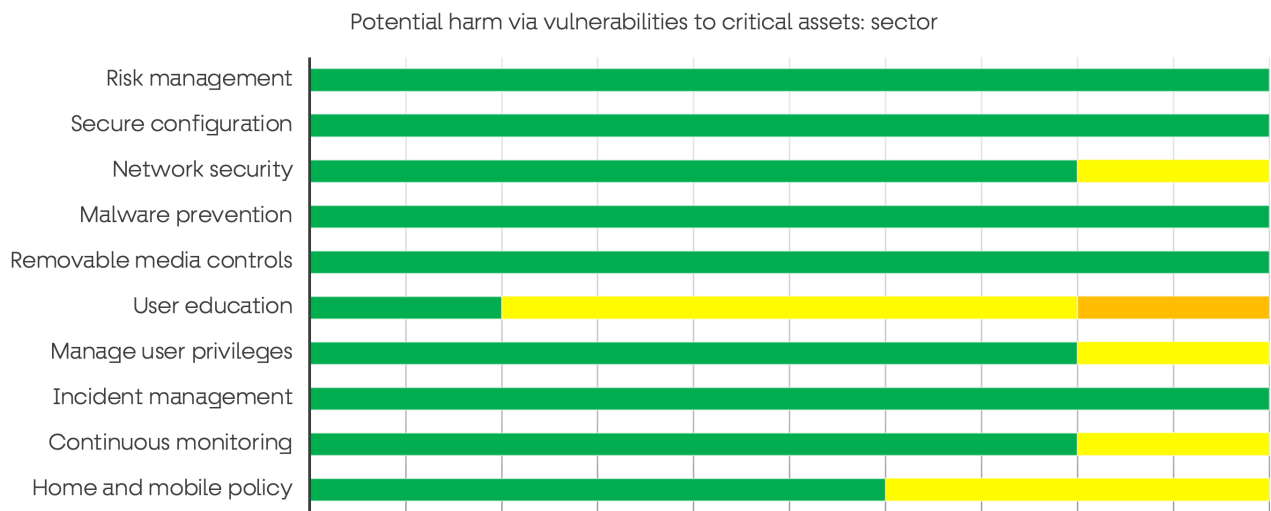


Figure 15: Private (Organisation) Sector's Vulnerabilities

The Private (Organisation) Sector appears exposed to exploits in user education, and home & mobile policy.

Private (Organisation) sector organisations should work on closing these weaknesses first, and then network security, incident management and continuous monitoring.

5.4. Impact of Private (Organisation) Sector Cyber Risks on Critical Services

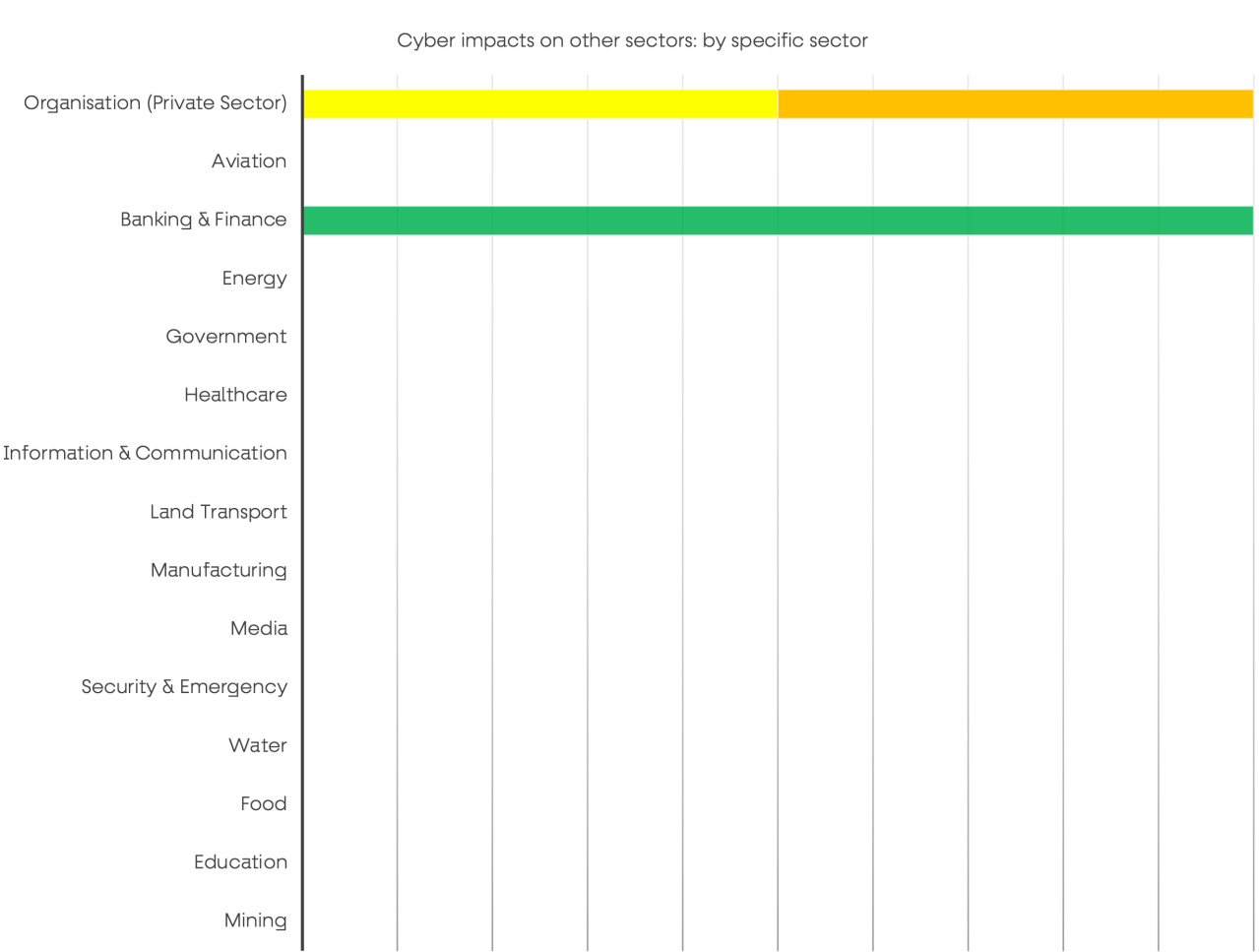


Figure 16: Sectors Impacted by Disruption in Private (Organisation) sector

The impacts from Private (Organisation) sector systems to other sectors are low to medium high with disruption to a low range of systems in other sectors.

It would be useful for Private (Organisation) sector organisations to understand their dependencies with systems in other Banking & Finance organisations. And then work out how follow-on impacts could be minimised.

6. Cyber Risk Posture in Critical Sectors: Aviation Sector

These are the analysed results and comments related to the Aviation Sector CII organisations. Overall there are no Aviation Sector CII systems in the high-risk zone that Cyber Criminals and Cyber Terrorists could attack using phishing and malware, through a range of vulnerabilities including weaknesses in risk management, secure configuration, network security and incident management. The impacts are quite minimal with a GDP impact of \$3,864,000 and disruption to other organisations in the Private (Organisation), Government and Land Transport sectors.

6.1. Threat Vectors of Concern to the Aviation Sector

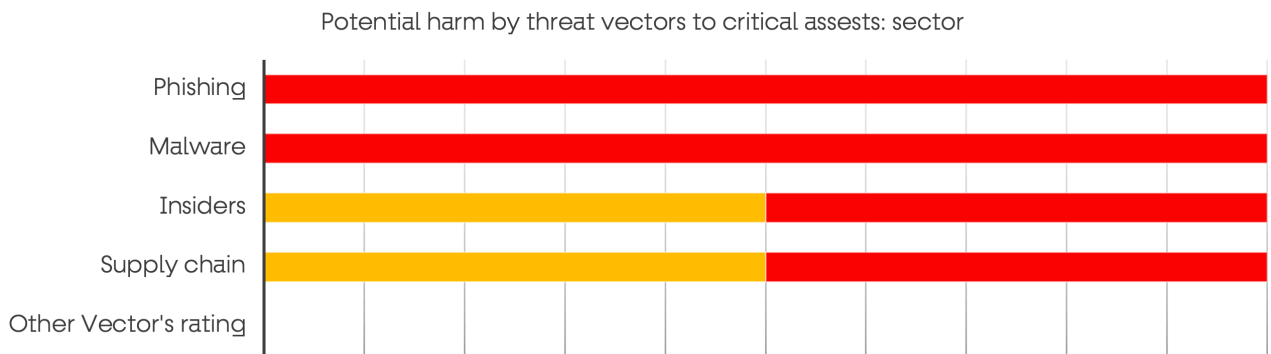


Figure 18: Aviation Sector's Threat Vectors

The greatest cyber threat vectors to Aviation sector CII systems are Malware and Phishing.

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

6.2. Threat Actors of Concern to The Aviation Sector

The greatest cyber threat vectors to Aviation sector CII systems are Malware and Phishing.

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

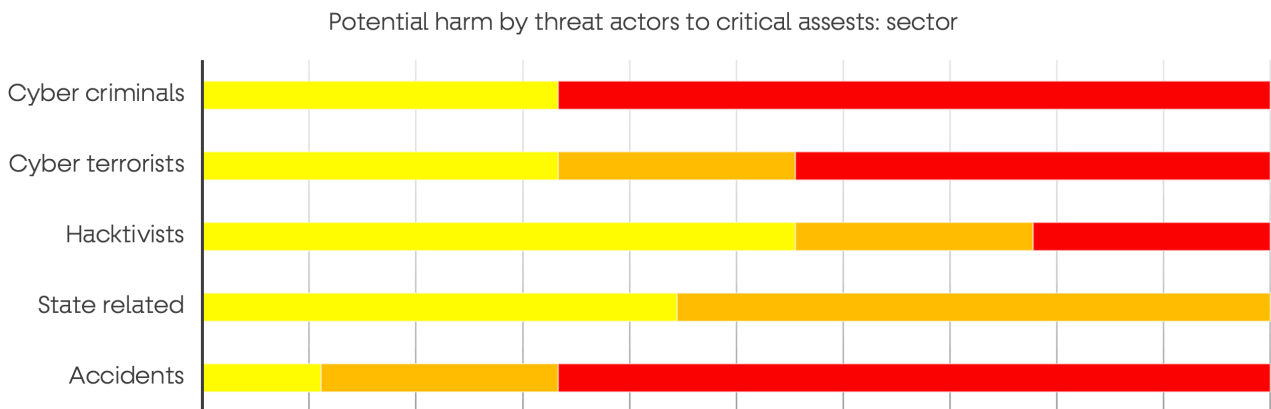


Figure 19: Aviation Sector's Threat Actors

By far the greatest cyber threat actor to Aviation sector CII systems are Cyber Criminals and Cyber Terrorists, with Hacktivists, State Related and Accidents a slightly lesser concern.

The Aviation sector's organisations should review the susceptibility of their systems to Cyber Criminals and Cyber Terrorists and determine how to detect and deter.

6.3. CII Vulnerabilities in the Aviation Sector

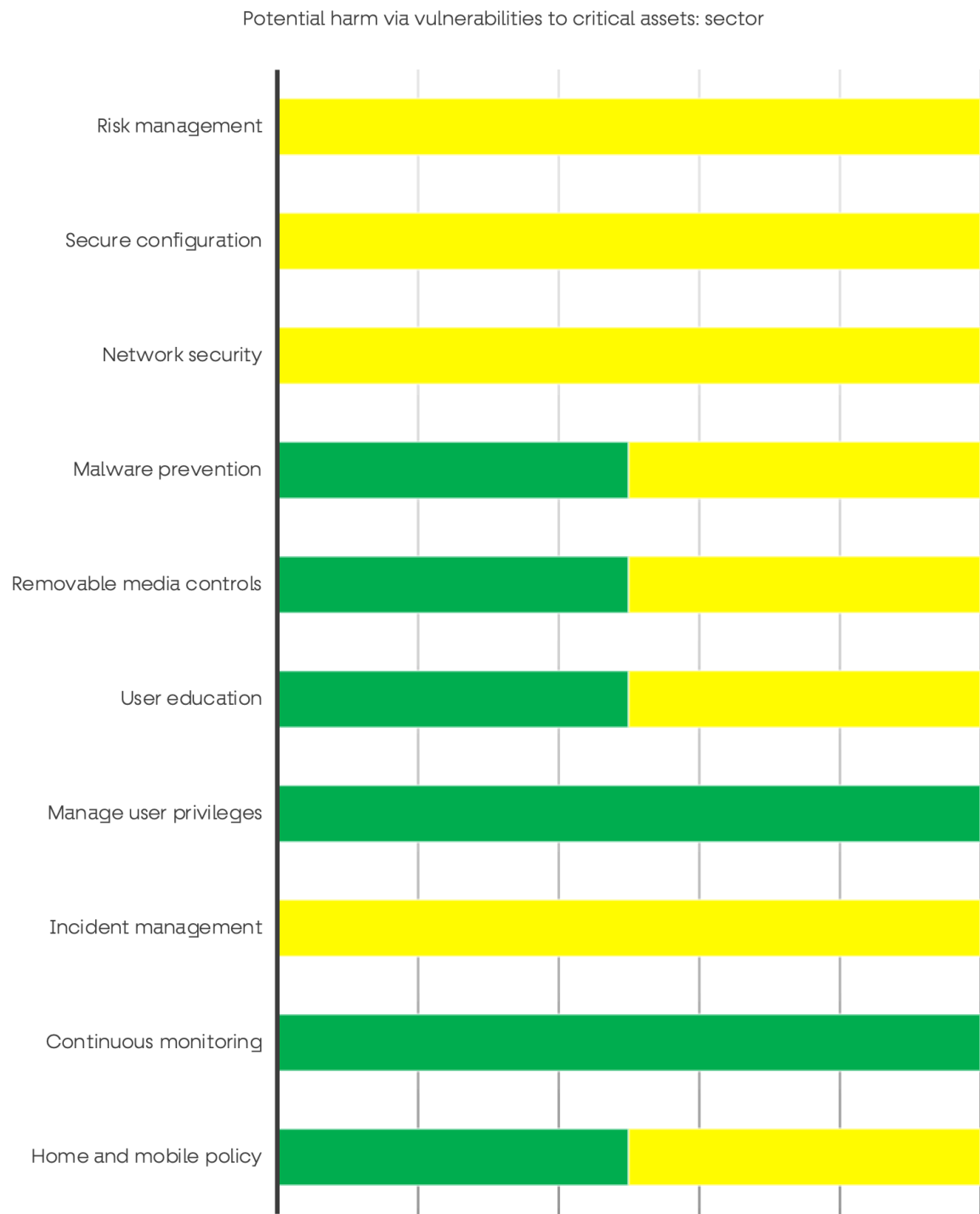


Figure 20: Aviation sector's Vulnerabilities

The Aviation sector appears exposed to exploits in risk management, secure configuration, network security and incident management.

Aviation sector organisations should work on closing these weaknesses first, and then malware prevention, removable media controls, user education and home and mobile policy.

6.4. Impact of Aviation Sector Cyber Risks on Critical Services

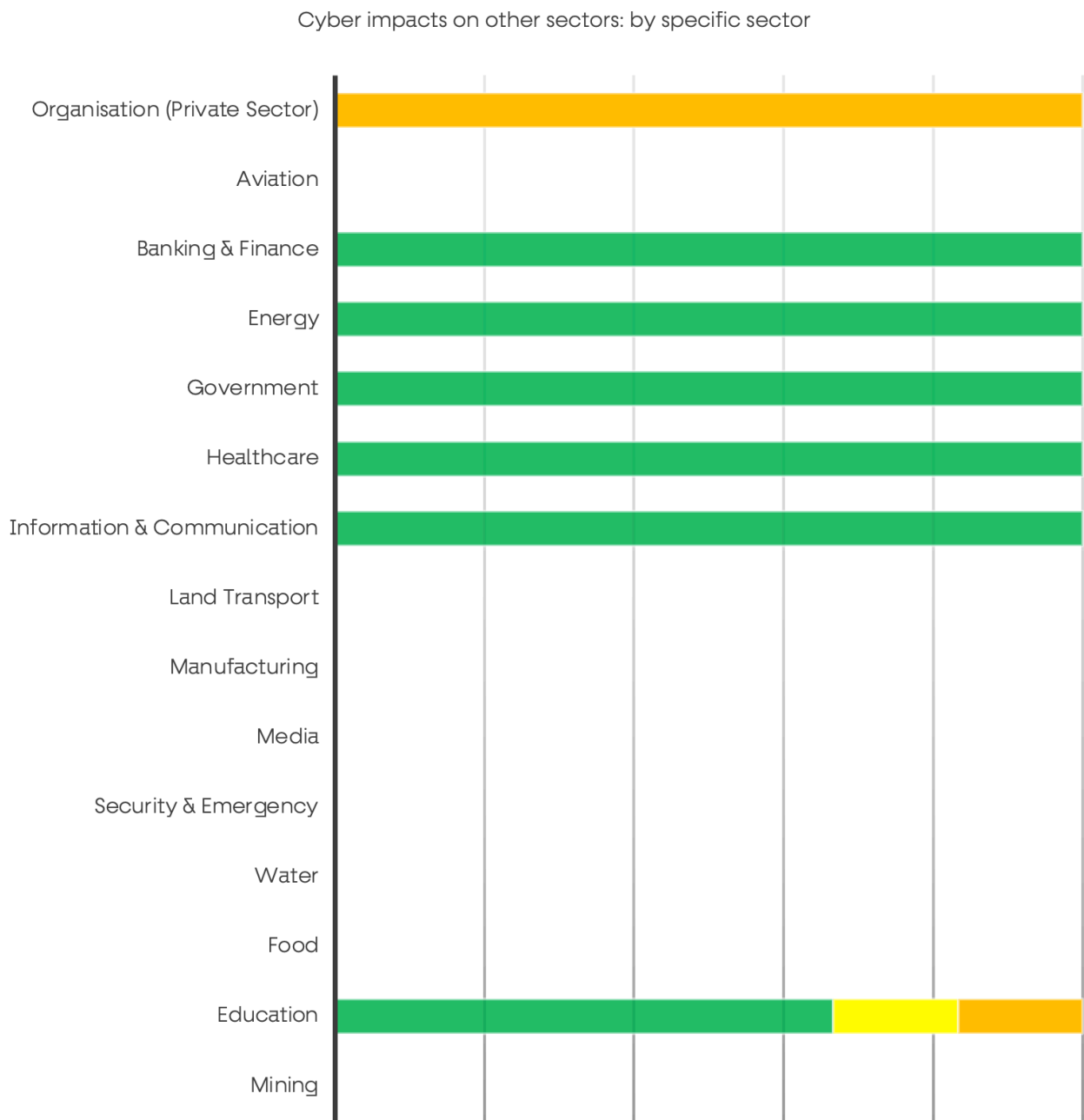


Figure 21: Sectors Impacted by Disruption in Aviation sector

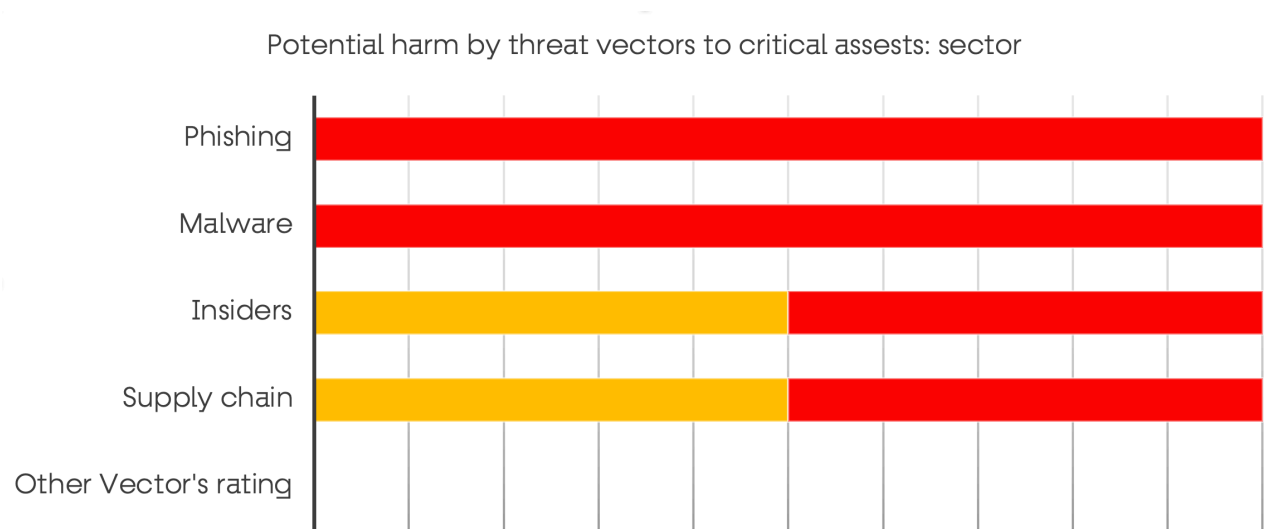
The impacts from Aviation sector systems to other sectors are low to medium high with disruption to a low range of systems in other sectors.

It would be useful for Aviation sector organisations to understand their dependencies with systems in other Private (Organisation), Banking & Finance, Government and Land Transport sectors. And then work out how follow-on impacts could be minimised.

7. Cyber Risk Posture in Critical Sectors: Banking & Finance Sector

These are the analysed results and comments related to the Banking & Finance Sector CII organisations. Overall there are 11 Banking & Finance Sector CII systems in the high-risk zone, that Cyber Criminals could attack using Phishing, through a range of vulnerabilities including weaknesses in user education. The impacts are quite significant with a GDP impact of \$2,351,244,000 and disruption to other organisations in the Private (Organisation), Government and Information & Communication sectors.

7.1. Threat Vectors of Concern to the Banking & Finance Sector



The greatest cyber threat vectors to Banking & Finance sector CII systems are Malware and Phishing. These should be investigated further with analysis of roles, processes, info and tools that could be used to reduce the threat from these vectors.

7.2. Threat Actors Of Concern to the Banking and Finance Sector

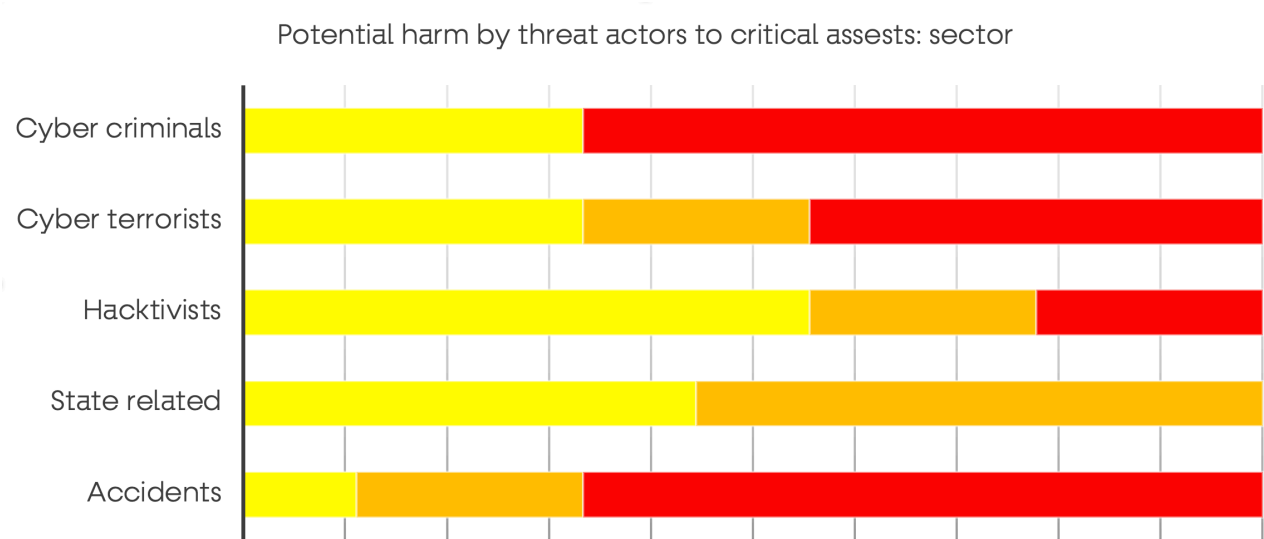


Figure 24: Banking & Finance Sector's Threat Actors

7.3. CII Vulnerabilities in the Banking & Finance Sector

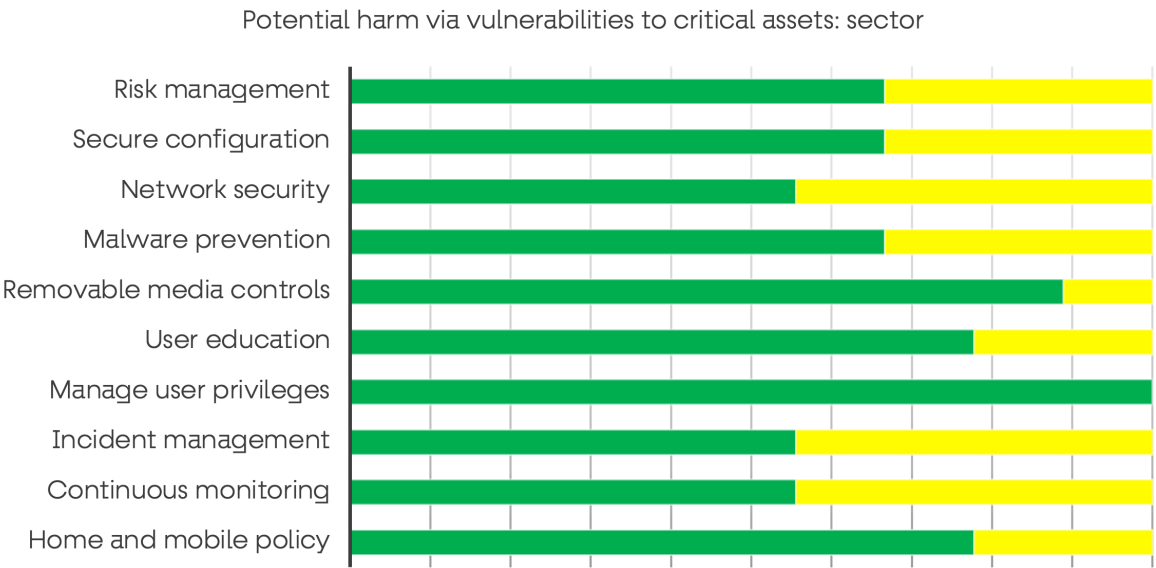


Figure 25: Banking & Finance Sector’s Vulnerabilities

The Banking & Finance sector appears exposed to significant weaknesses in user education, manage user privileges and secure configurations.

Banking & Finance sector organisations should work on closing these weaknesses first, and then network security, continuous monitoring and risk management.

7.4. Impact of Banking and Finance Sector Cyber Risks on Critical Services

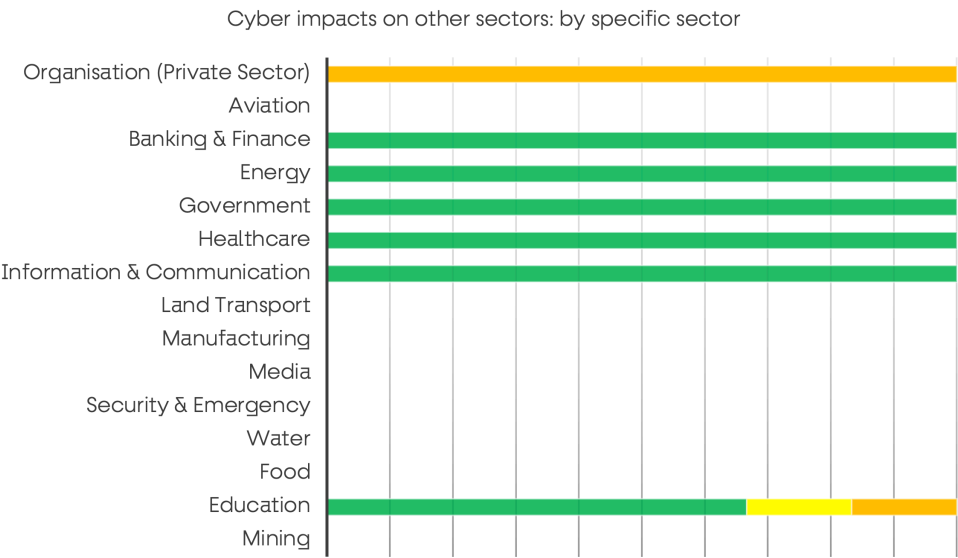


Figure 26: Sectors Impacted by Disruption in Banking & Finance Sector

The impacts from Banking & Finance sector systems to other sectors are low to medium high with disruption to a wide range of systems in other sectors.

It would be useful for Banking & Finance sector organisations to understand their dependencies with systems in other organisations in all the other sectors. And then work out how follow-on impacts could be minimised.

8. Cyber Risk Posture in Critical Sectors: Energy Sector

These are the analysed results and comments related to the Energy Sector CII organisations. Overall there are no CII systems in the high-risk zone, that Cyber Criminals could attack using Malware, through a range of vulnerabilities including weaknesses in Malware Prevention. The impacts are quite minimal with a GDP impact of \$202,860,000 and disruption to other

8.1. THREAT VECTORS OF CONCERN TO THE ENERGY SECTOR

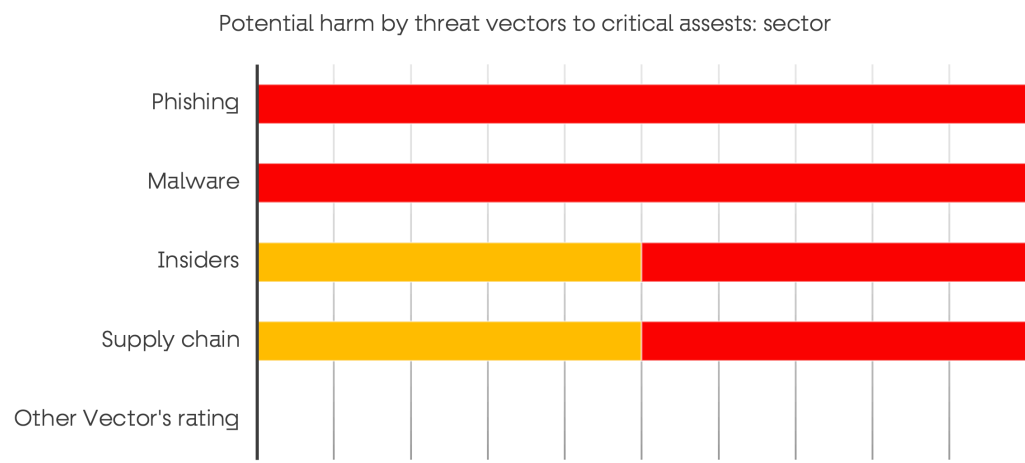


Figure 28: Energy Sector's Threat Vectors

The greatest cyber threat vectors to Energy sector CII systems are Malware and Phishing.

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

8.2. Threat Actors of Concern to the Energy Sector

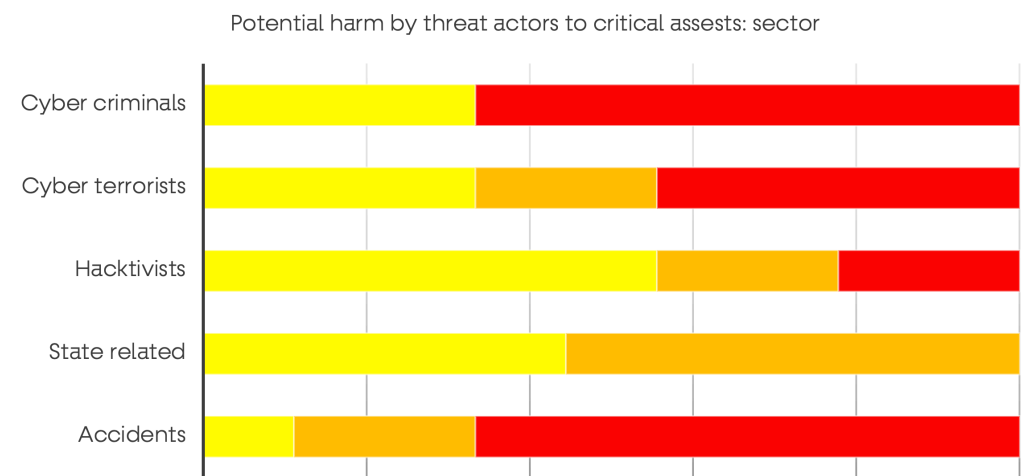


Figure 29: of Energy Sector's Threat Actors

8.3. CII Vulnerabilities in the Energy Sector

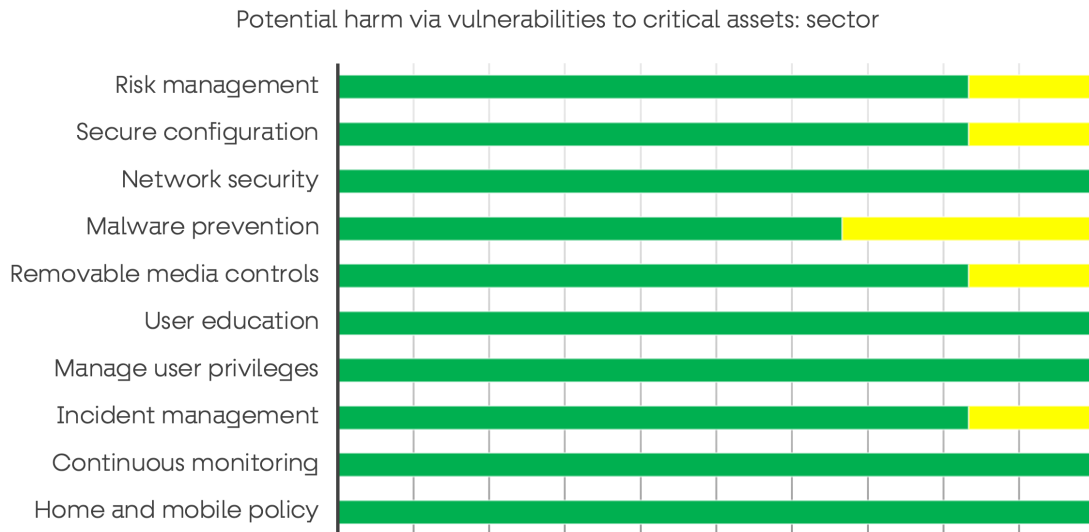


Figure 30: Energy Sector's Vulnerabilities

The Energy sector appears exposed to exploits in malware prevention.

Energy sector organisations should work on closing these weaknesses first, and then risk management, secure configuration, removable media controls and incident management.

8.4. Impact of Energy Sector Cyber Risks on Critical Services

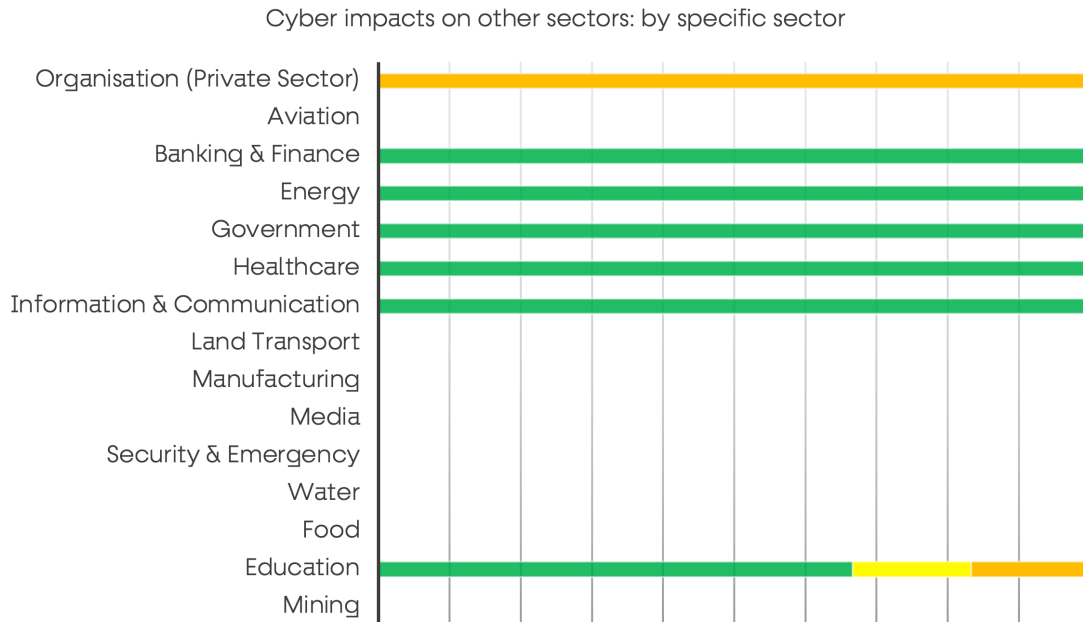


Figure 31: Sectors Impacted by Disruption in Energy Sector

The impacts from Energy sector systems to other sectors are low to medium high with disruption to a medium range of systems in other sectors.

It would be useful for Energy sector organisations to understand their dependencies with systems in other organisation in the Private (Organisation), Government, Information & Communication, Security and Emergency, Water and Mining sectors. And then work out how follow-on impacts could be minimised.

9. Cyber Risk Posture in Critical Sectors: Government Sector

These are the analysed results and comments related to the Government sector CII organisations. Overall there is 1 Government sector CII systems in the high-risk zone, that Cyber Criminals could attack using Malware, through a range of vulnerabilities including weaknesses in removable media controls. The impacts are quite significant with a GDP impact of \$1,903,020,000 and disruption to other organisations in the Information & Communication, Security and Emergency and Healthcare sectors.

9.1. Threat Vectors Of Concern To The Government Sector

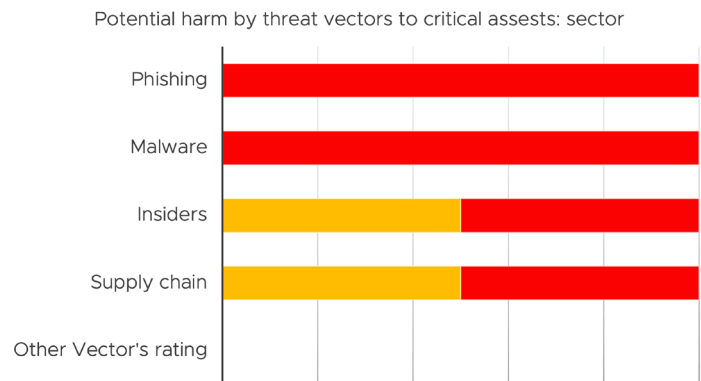


Figure 33: Government Sector's Threat Vectors

The greatest cyber threat vectors to Government sector CII systems are Malware and Phishing.

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

9.2. Threat Actors of Concern to the Government Sector

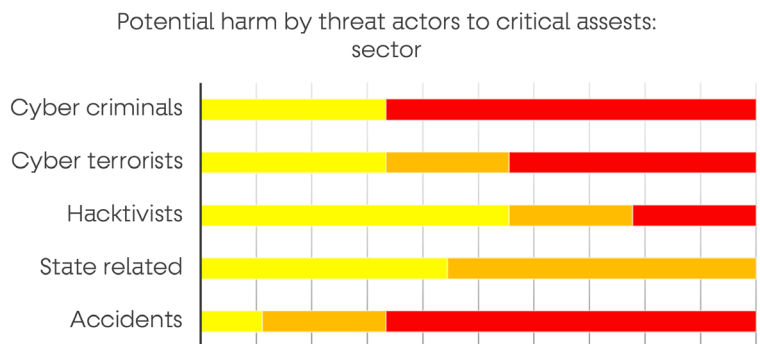


Figure 34: Government Sector's Threat Actors

By far the greatest cyber threat actor to Government sector CII systems is Cyber Criminals, with State Related a slightly lesser concern.

The Government sector's organisations should review the susceptibility of their systems to Cyber Criminals and determine how to detect and deter.

9.3. CII Vulnerabilities in the Government Sector

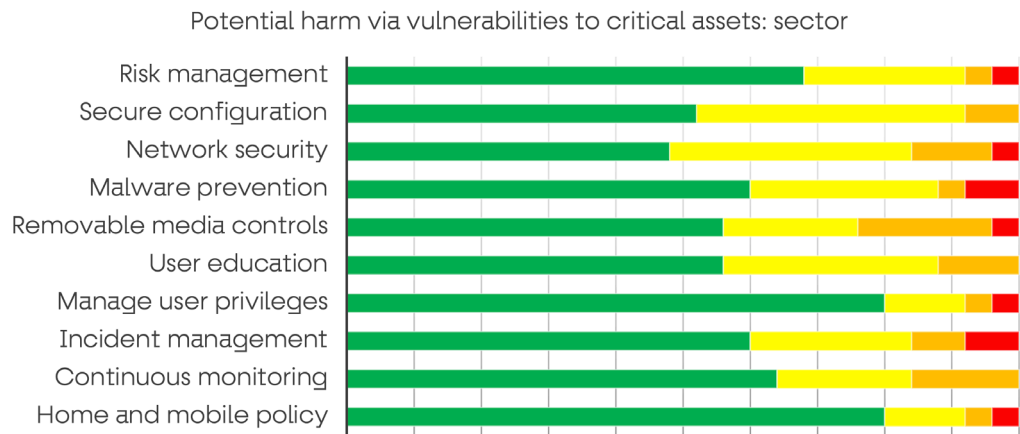


Figure 35: Government Sector's Vulnerabilities

The Government sector appears exposed to extreme weaknesses in incident management, malware prevention, network security, managing user privileges, and removable media controls.

Government sector organisations should work on closing these weaknesses first, and then network security, user education and continuous monitoring.

9.4. Impact of Government Sector Cyber Risks on Critical Services

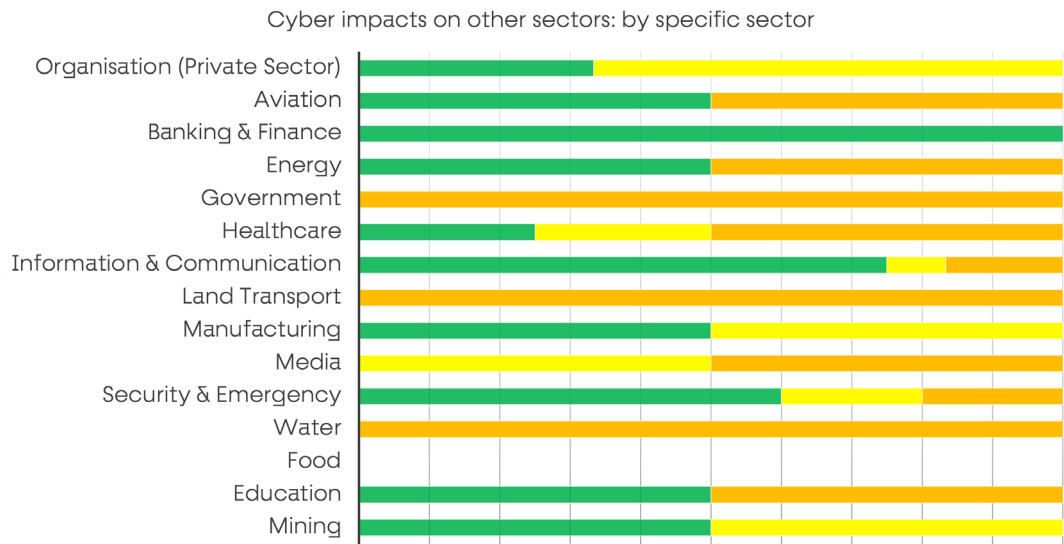


Figure 36: Sectors Impacted by Disruption in Government Sector

The impacts from Government sector systems to other sectors are low to medium high with disruption to a wide range of systems in other sectors.

It would be useful for Government sector organisations to understand their dependencies with systems in other organisations in all sectors. And then work out how follow-on impacts could be minimised.

10. Cyber Risk Posture in Critical Sectors: Healthcare Sector

These are the analysed results and comments related to the Healthcare sector CII organisations. Overall there are 6 Healthcare sector CII systems in the high-risk zone, that Cyber Criminals could attack using Malware, through a range of vulnerabilities including weaknesses in removable media controls and malware prevention. The impacts are quite significant with a GDP impact of \$989,184,000 and disruption to other organisations in the Government, Information & Communication and Private (Organisation) sectors.

10.1. Threat Vectors of Concern to the Healthcare Sector

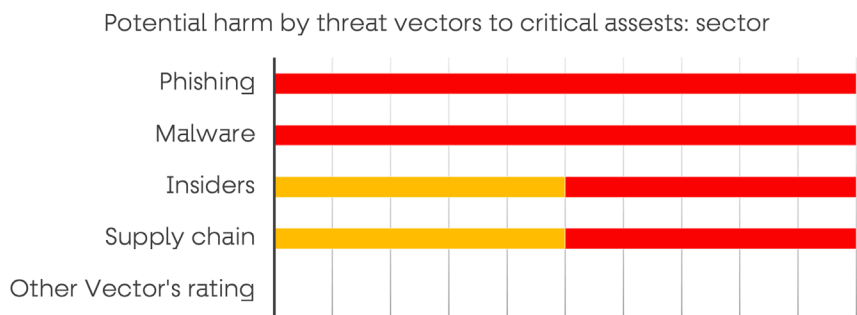


Figure 38: Healthcare Sector's Threat Vectors

The greatest cyber threat vectors to Healthcare sector CII systems are Malware and Phishing.

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

10.2. Threat Actors of Concern to the Healthcare Sector

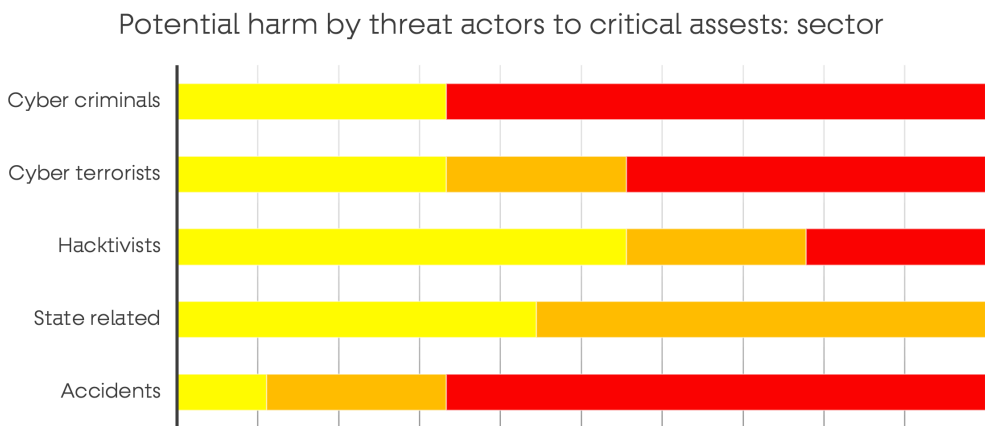


Figure 39: Healthcare Sector's Threat Actors

By far the greatest cyber threat actor to Healthcare sector CII systems is Cyber Criminals, with Hacktivists a slightly lesser concern.

The Healthcare sector’s organisations should review the susceptibility of their systems to Cyber Criminals and determine how to detect and deter.

10.3. CII Vulnerabilities in the Healthcare Sector

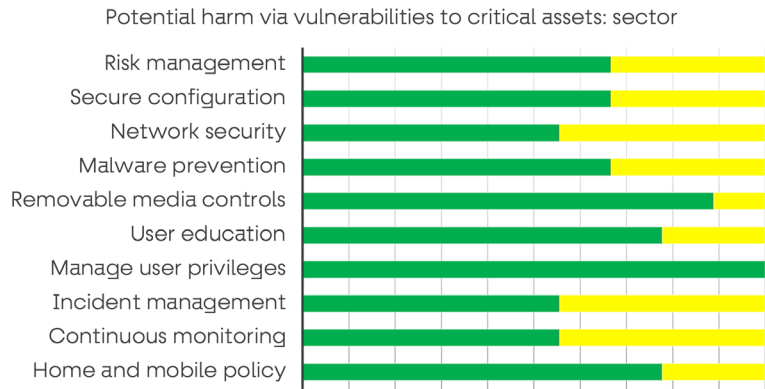


Figure 40: Healthcare Sector’s Vulnerabilities

The Healthcare sector appears exposed to extreme weaknesses in removable media controls, malware prevention and network security.

Healthcare sector organisations should work on closing these weaknesses first, and then continuous monitoring, risk management and user education.

10.4. Impact of Healthcare Sector Cyber Risks on Critical Services



Figure 41: Sectors Impacted by Disruption in Healthcare Sector

The impacts from Healthcare sector systems to other sectors are low to medium high with disruption to a wide range of systems in other sectors.

It would be useful for Healthcare sector organisations to understand their dependencies with systems in other organisations of all sectors. And then work out how follow-on impacts could be minimised.

11. Cyber Risk Posture in Critical Sectors: Information & Communication Sector

These are the analysed results and comments related to the Information & Communication sector CII organisations. Overall there are 13 Information & Communication sector CII systems in the high-risk zone, that Cyber Criminals could attack using malware and phishing, through a range of vulnerabilities including weaknesses in user education. The impacts are quite minimal with a GDP impact of \$488,796,000 and disruption to other organisation in the Private (Organisation), Government and Banking & Finance sectors.

11.1. Threat Vectors of Concern to the Information & Communication Sector

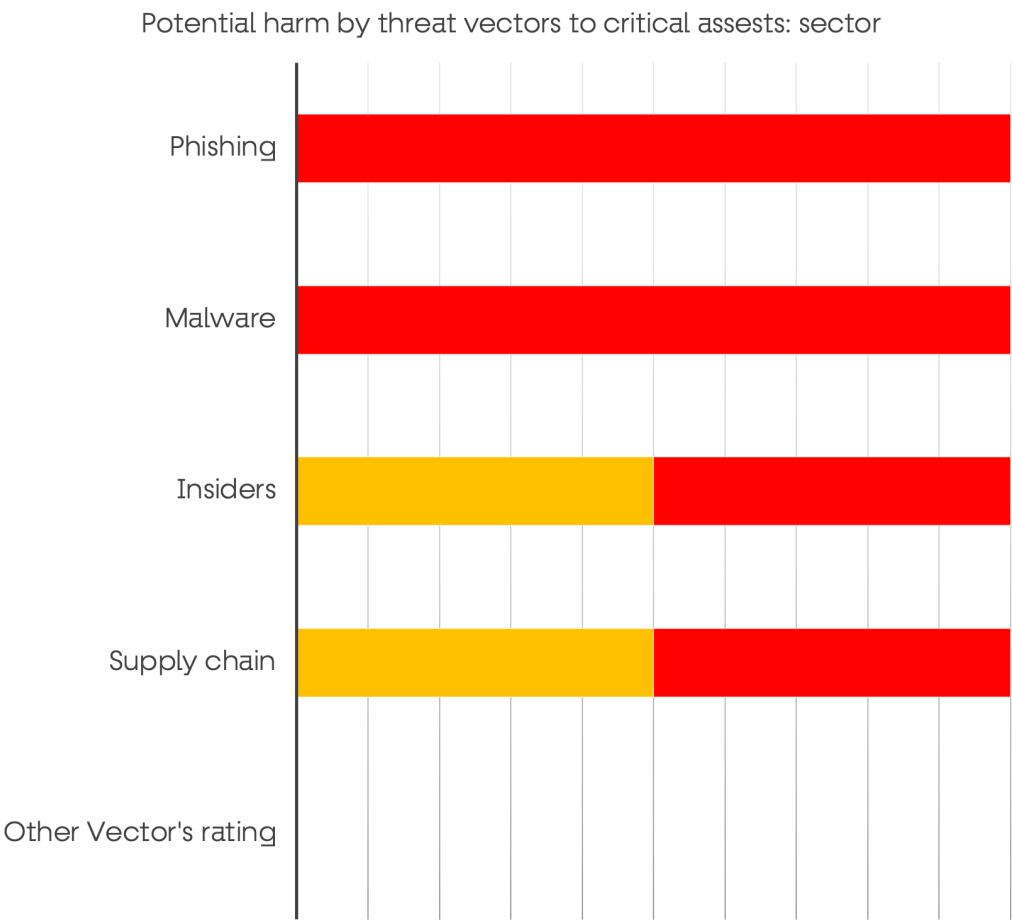


Figure 43: Information & Communication Sector's Threat Vectors

The greatest cyber threat vectors to Information & Communication sector CII systems are Malware and Phishing.

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

11.2. Threat Actors of Concern to the Information and Communication Sector

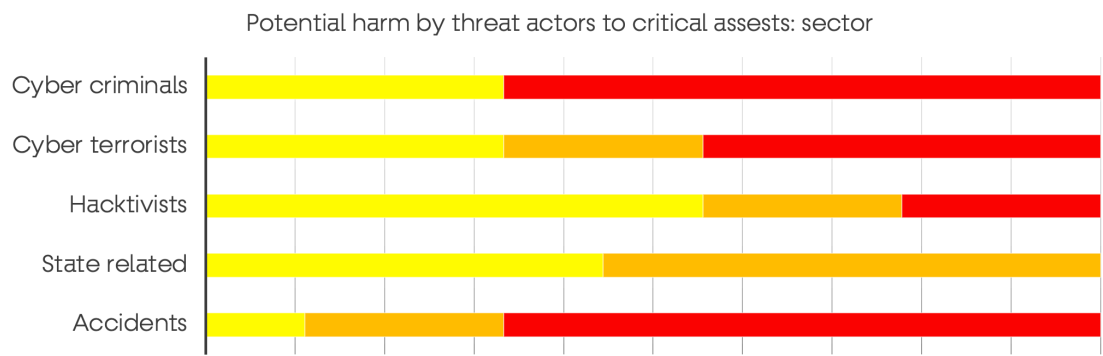


Figure 44: Information & Communication Sector’s Threat Actors

By far the greatest cyber threat actor to Information & Communication sector CII systems is Cyber Criminals, with Cyber Terrorists a slightly lesser concern.

The Information & Communication sector’s organisations should review the susceptibility of their systems to Cyber Criminals and determine how to detect and deter.

11.3. CII VULNERABILITIES IN THE INFORMATION & COMMUNICATION SECTOR

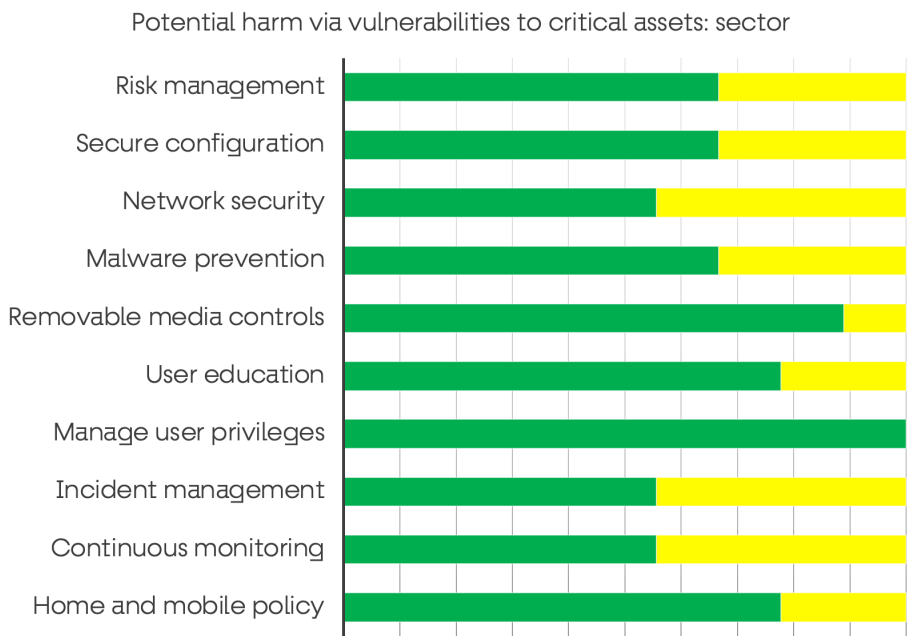


Figure 45: Information & Communication Sector’s Vulnerabilities

The Information & Communication sector appears exposed to exploits in user education, malware prevention and network security.

Information & Communication sector organisations should work on closing these weaknesses first, and then secure configuration, continuous monitoring and incident management.

11.4. Impact of Information & Communication Sector Cyber Risks on Critical Services

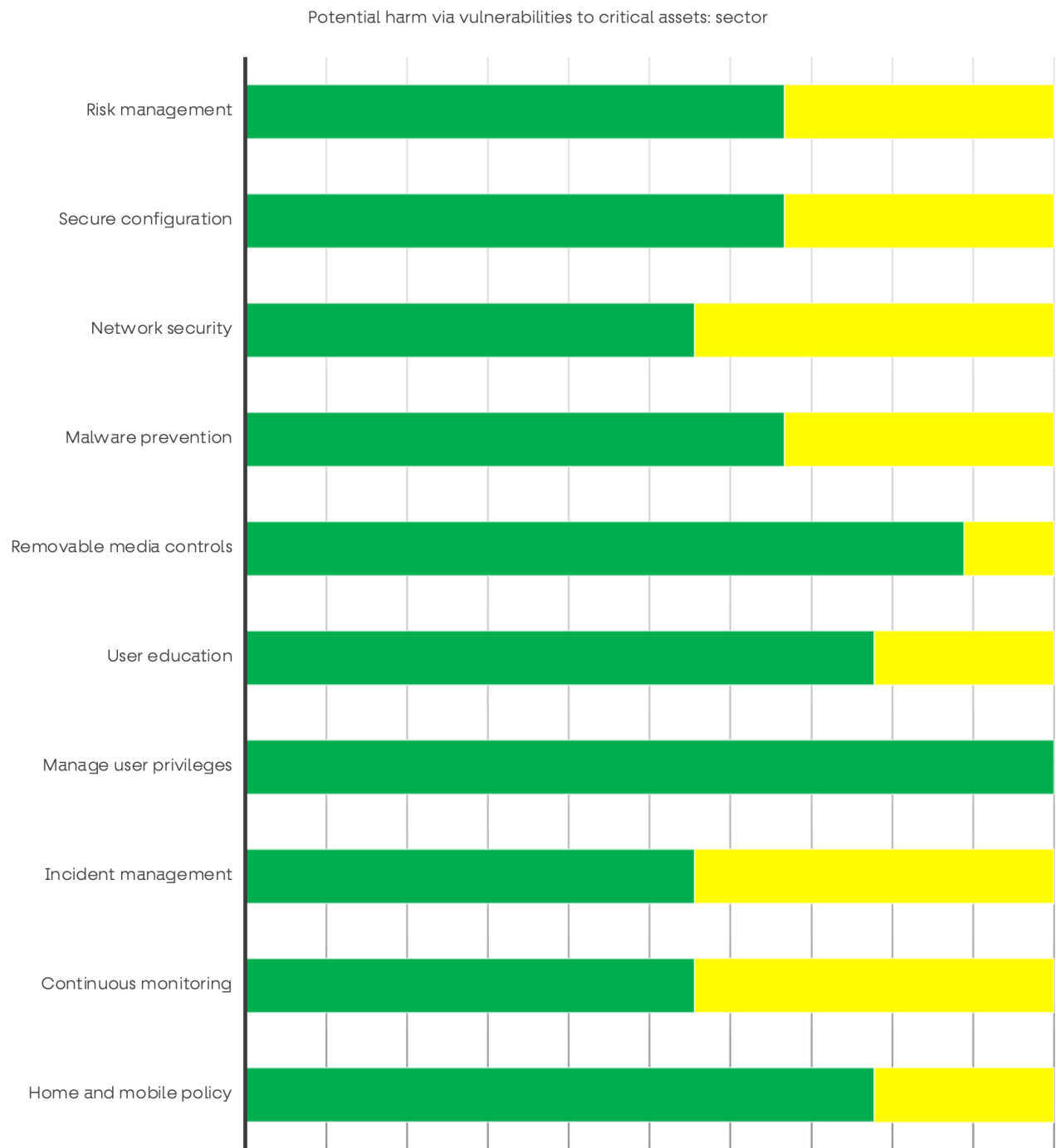


Figure 46: Sectors Impacted by Disruption in Information & Communication Sector

The impacts from Information & Communication sector systems to other sectors are low to medium high with disruption to a wide range of systems in other sectors.

It would be useful for Information & Communication sector organisations to understand their dependencies with systems in other organisations in all other sectors. And then work out how follow-on impacts could be minimised.

12. Cyber Risk Posture in Critical Sectors: Land and Transport Sector

These are the analysed results and comments related to the Land & Transport sector CII organisations. Overall there is 1 Land & Transport sector CII system in the high-risk zone, that Cyber Criminals could attack using Malware and Insiders, through a range of vulnerabilities including weaknesses in malware prevention. The impacts are minimal with a GDP impact of \$19,320,000 and disruption to other organisations in the Aviation and Manufacturing sectors.

12.1. Threat Vectors of Concern to the Land and Transport Sector

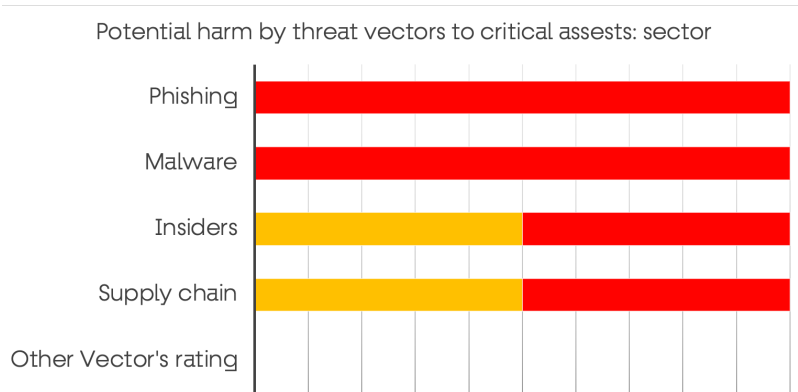


Figure 48: Land & Transport Sector's Threat Vectors

The greatest cyber threat vectors to Land & Transport sector CII systems are Malware and Insiders.

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

12.2. Threat Actors of Concern to the Land and Transport Sector

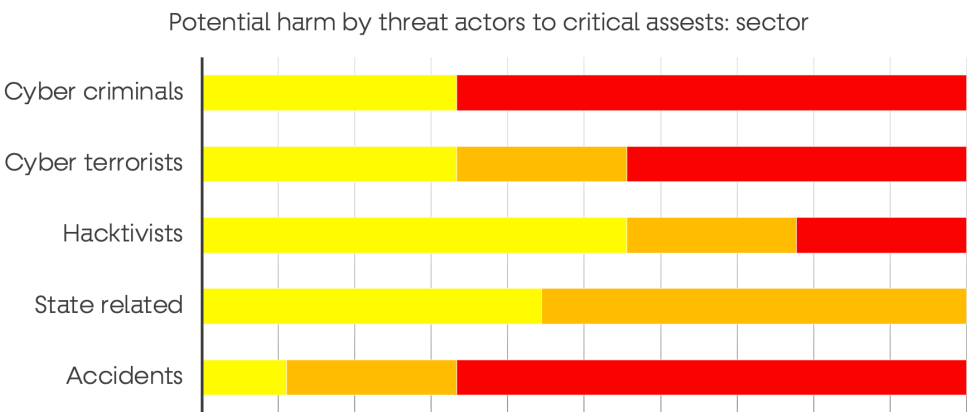


Figure 49: Land & Transport Sector's Threat Actors

By far the greatest cyber threat actor to Land & Transport sector CII systems is Cyber Criminals, with State Related and Accidents a slightly lesser concern.

The Land & Transport sector's organisations should review the susceptibility of their systems to Cyber Criminals and determine how to detect and deter.

12.3. CII Vulnerabilities in the Land & Transport Sector



Figure 50: Land & Transport Sector’s Vulnerabilities

The Land & Transport sector appears exposed to exploits in malware prevention.

Land & Transport sector organisations should work on closing these weaknesses first, and then risk management, network security, incident management and continuous monitoring.

12.4. Impact of Land and Transport Sector Cyber Risks on Critical Services

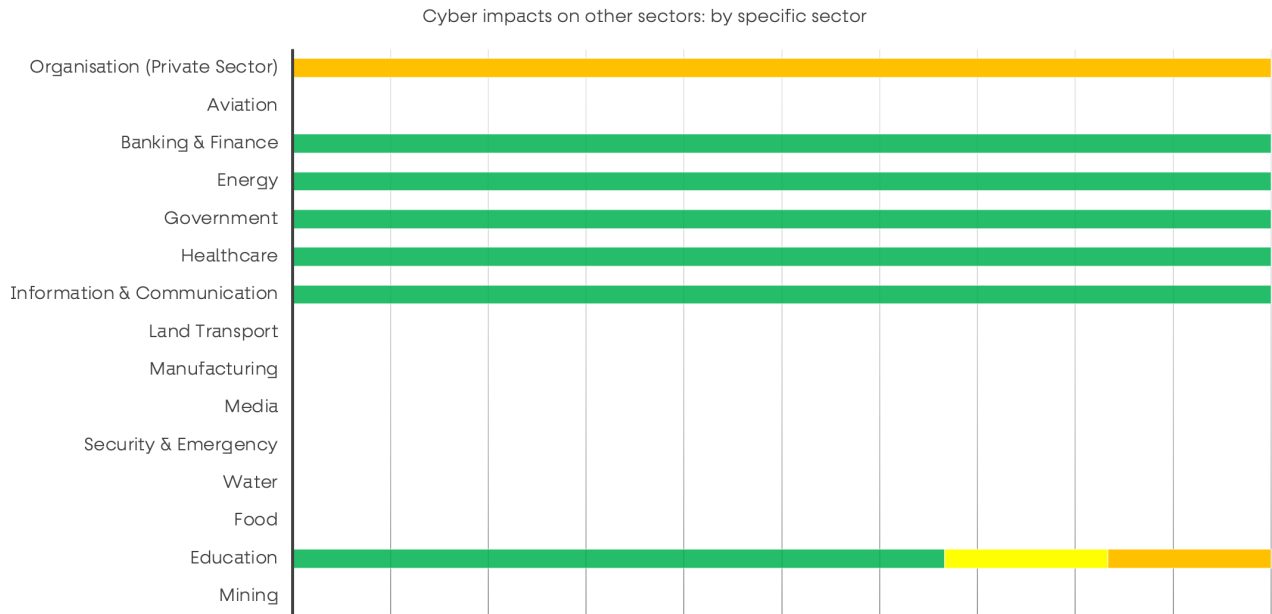


Figure 51: Sectors Impacted by Disruption in Land & Transport Sector

The impacts from Land & Transport sector systems to other sectors are of medium significance with disruption to a low range of systems in other sectors.

It would be useful for Land & Transport sector organisations to understand their dependencies with systems in other organisations in the Aviation and Manufacturing sector. And then work out how follow-on impacts could be minimised.

13. Cyber Risk Posture in Critical Sectors: Water Sector

These are the analysed results and comments related to the Water sector CII organisations. Overall there are no Water sector CII systems in the high-risk zone, that Cyber Criminals could attack using Malware, through a range of vulnerabilities including weaknesses in user education. The impacts are minimal with a GDP impact of \$11,592,000 and disruption to other organisations in the Mining, Private (Organisation) and Government sectors.

13.1. Threat Vectors of Concern to the Water Sector

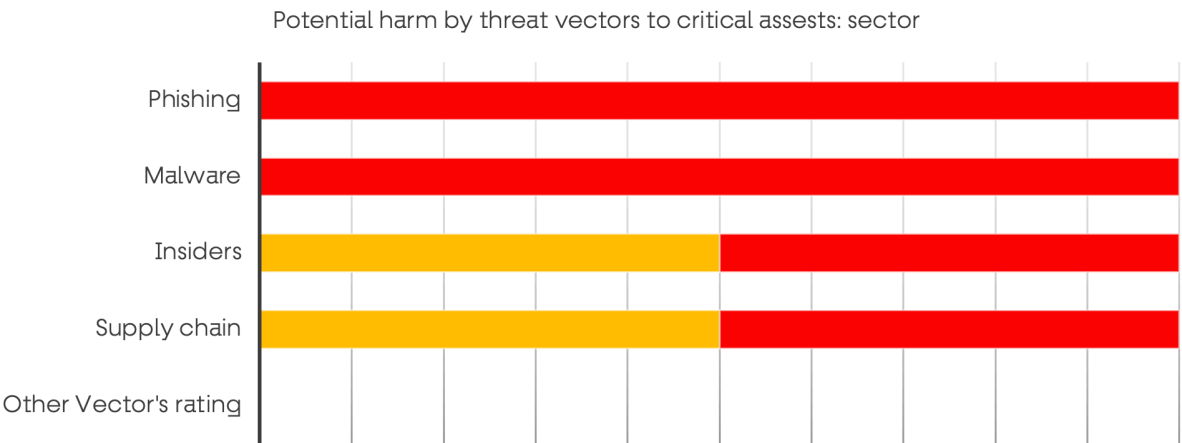


Figure 53: Water Sector's Threat Vectors

The greatest cyber threat vectors to Water sector CII systems is Malware.

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

13.2. Threat Actors of Concern to the Water Sector

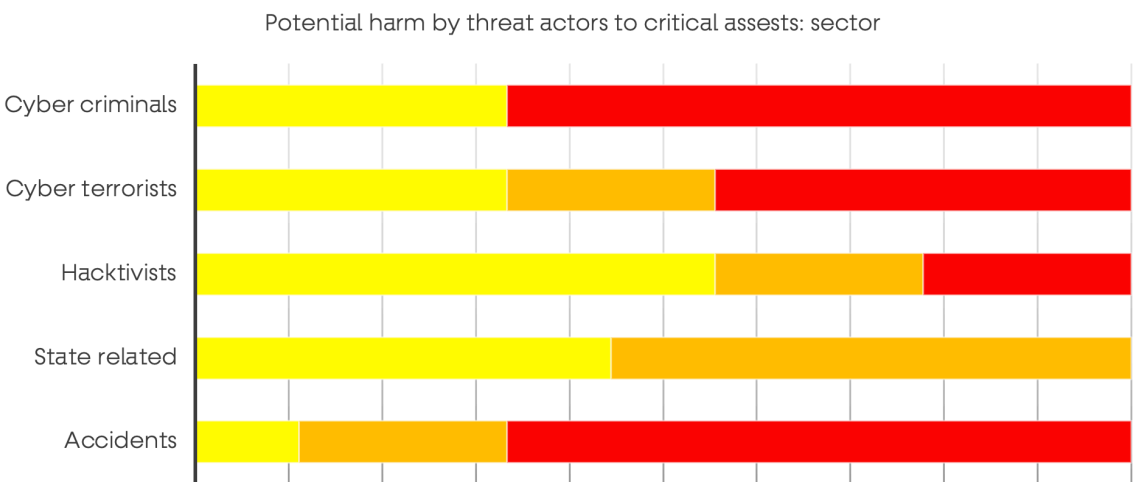


Figure 54: Water Sector's Threat Actors

By far the greatest cyber threat actor to Water sector CII systems is Cyber Criminals, with Cyber Terrorists, Hacktivists, State Related and Accidents a slightly lesser concern.

The Water sector's organisations should review the susceptibility of their systems to Cyber Criminals and determine how to detect and deter.

13.3. CII Vulnerabilities in the Water Sector

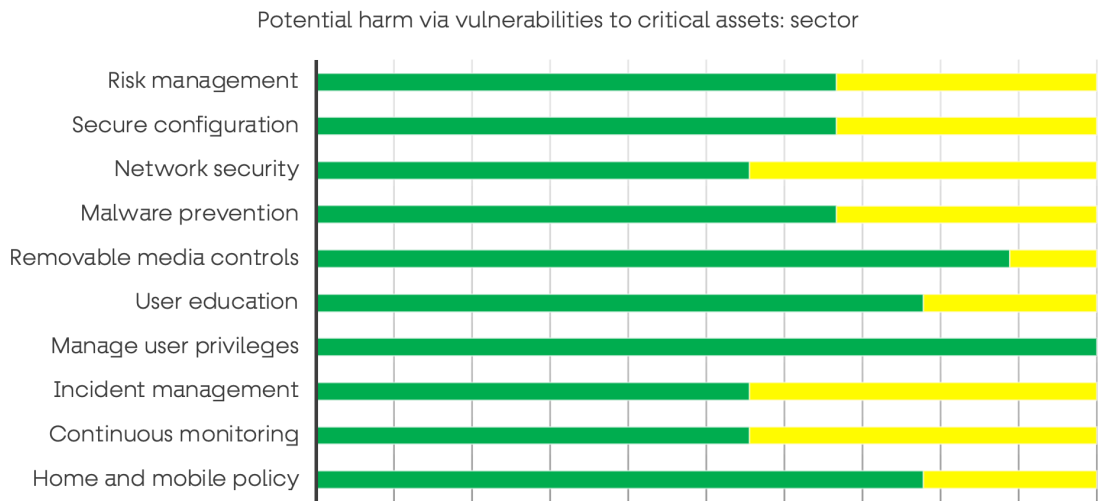


Figure 55: Water Sector's Vulnerabilities

The Water sector appears exposed to exploits in user education, secure configuration and continuous monitoring.

Water sector organisations should work on closing these weaknesses first, and then malware prevention and risk management.

13.4. Impact of Water Sector Cyber Risks on Critical Services

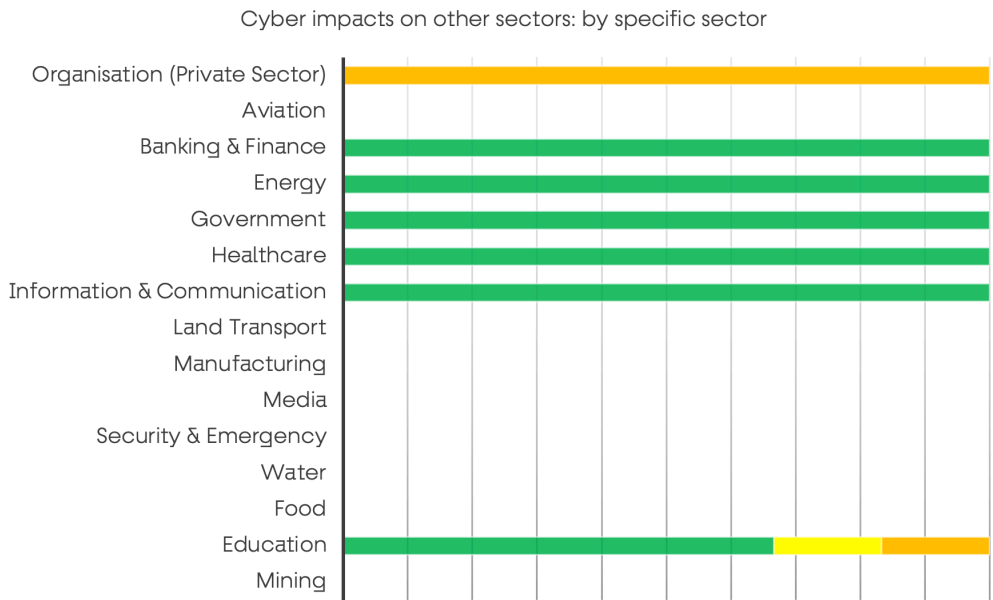


Figure 56: Sectors Impacted by Disruption in Water Sector

The impacts from Water sector systems to other sectors are low to medium high with disruption to a medium range of systems in other sectors.

It would be useful for Water sector organisations to understand their dependencies with systems in other organisations of Mining, Food, Manufacturing, Information & Communication, Healthcare, Government, Aviation and Private (Organisation) sector. And then work out how follow-on impacts could be minimised.

14. Cyber Risk Posture in Critical Sectors: Water Sector

These are the analysed results and comments related to the Education sector CII organisations. Overall there are no Education sector CII systems in the high-risk zone, that Cyber Criminals and Accidents could attack using Insiders and Malware, through a range of vulnerabilities including weaknesses in network security, incident management and continuous monitoring. The impacts are minimal with a GDP impact of \$17,388,000 and disruption to other organisations in the Private (Organisation) and Government.

14.1. Threat Vectors of Concern to the Education Sector

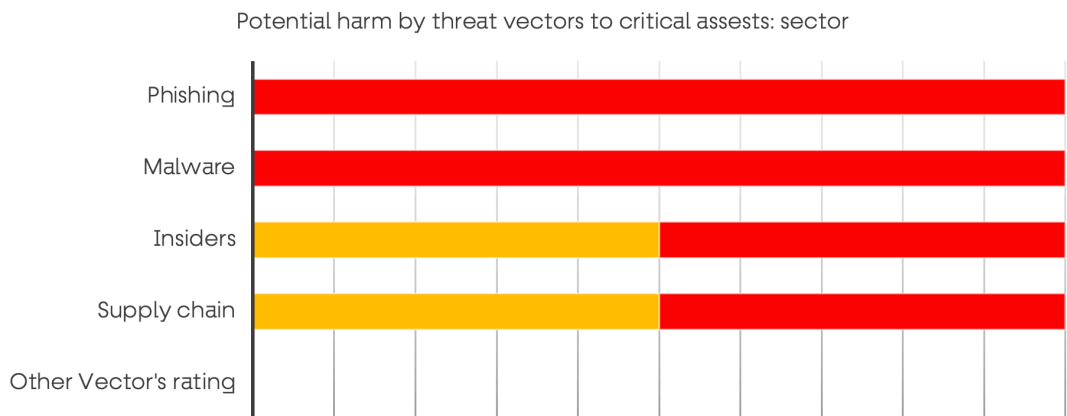


Figure 58: Education Sector's Threat Vectors

The greatest cyber threat vectors to Education sector CII systems are Insiders.

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

14.2. Threat Actors of Concern to the Education Sector

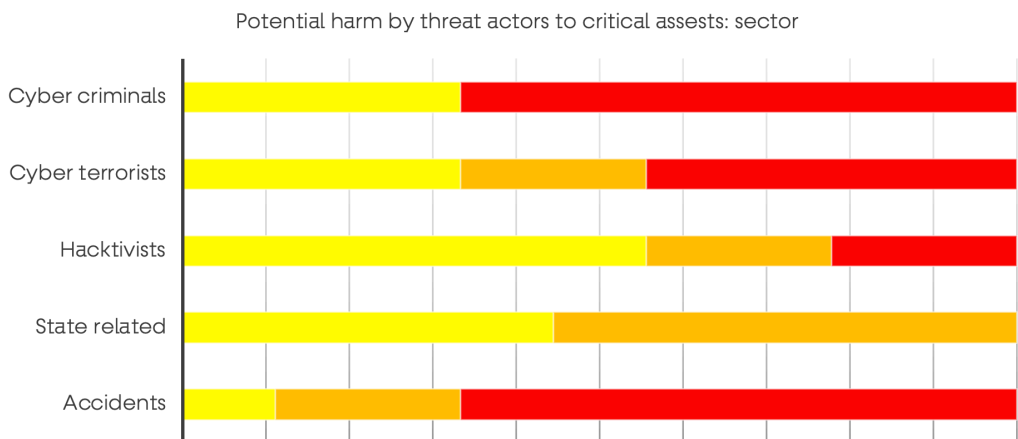


Figure 59: Education Sector's Threat Actors

By far the greatest cyber threat actor to Education sector CII systems is Accidents, with Cyber Criminals a slightly lesser concern.

The Education sector's organisations should review the susceptibility of their systems to Accidents and determine how to detect and deter.

14.3. CII Vulnerabilities in the Education Sector

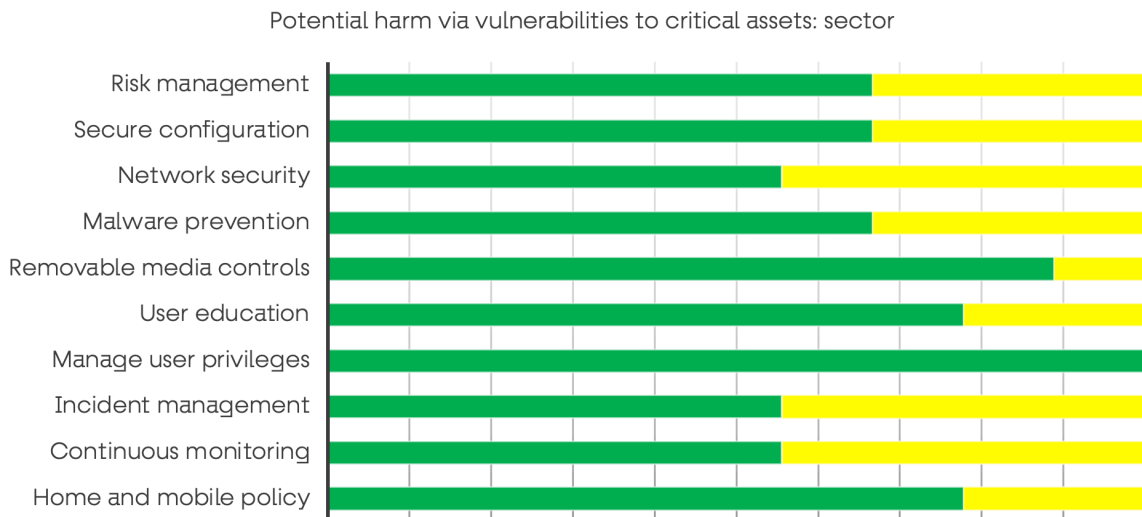


Figure 60: Education Sector's Vulnerabilities

The Education sector appears exposed to exploits in continuous monitoring, incident management and network security.

Education sector organisations should work on closing these weaknesses first, and then risk management, secure configuration and malware prevention.

14.4. Impact of Education Sector Cyber Risks on Critical Services

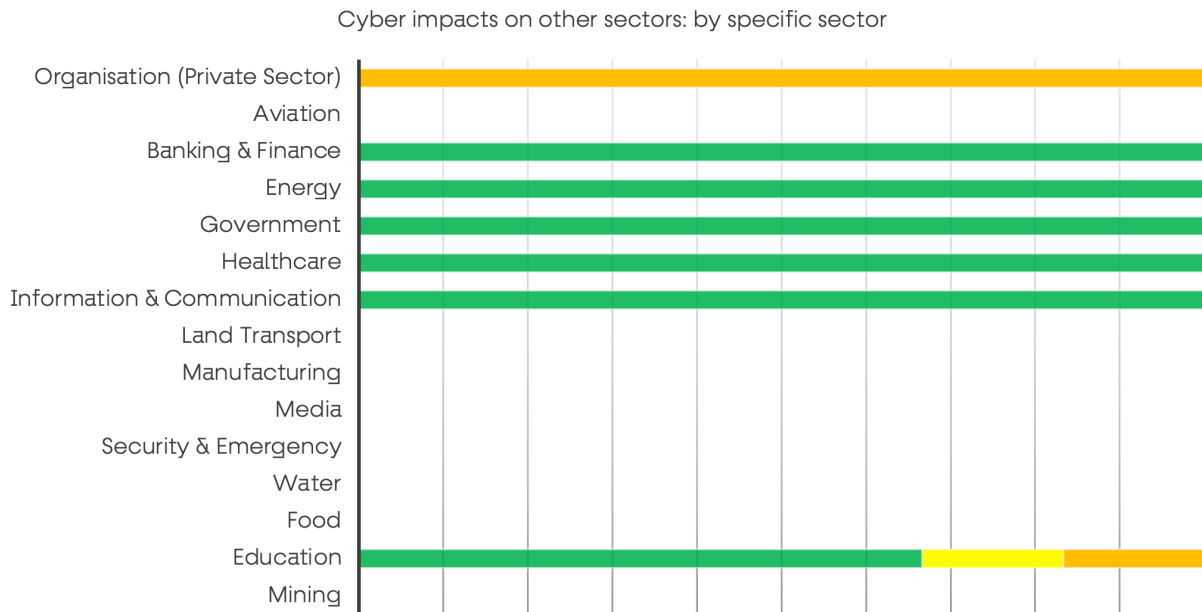


Figure 61: Sectors Impacted by Disruption in Education Sector

The impacts from Education sector systems to other sectors are low to medium high with disruption to a medium range of systems in other sectors.

It would be useful for Education sector organisations to understand their dependencies with systems in other organisations in the Information & Communication, Healthcare, Government, Energy, Banking & Finance and Private (Organisation) sectors. And then work out how follow-on impacts could be minimised.

Recommendations

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, ZICTA, or some joint activity. Recommendations presented here will be taken forward for review in Zambia's next cyber strategy, and existing and new cyber capability and capacity building projects / initiatives as necessary.

Recommendation 1:

CII organisations should 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 Authority works in partnership with those organisations owning the most critical systems to help develop minimum standards for enhanced cyber security. Note that this could be through (a) reductions in impact, possibly through redesign of the 'reach' of systems; and through (b) the likelihood of attack, through improvements in control usage and other vulnerability reductions.

Recommendation 2:

CII organisations should 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, cyber-attack simulations/exercises, and analysis of their logs for signs of reconnaissance, probing and exploits. Consider also the establishment of secure cyber information sharing mechanisms for organisations within and across sectors. This could be via a central platform, or be based on organisation-to-organisation relationships and secure messaging apps e.g. Signal, Telegram, etc.

Recommendation 3:

CII organisations should reduce specific vulnerabilities. A standard package of advice and guidance based on the Cyber Security Baseline Controls Guideline, system audit/testing and adopting minimum cyber security standards should all be considered. Ultimately, CII organisations should be setting the standard for cyber security amongst businesses, with minimal vulnerabilities, and use of rigorous control regimes.

Recommendation 4

CII organisations should 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. This will improve user responses and reduce accidents.

Recommendation 5:

CII organisations should 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 6:

The Authority will consider undertaking the following:

- Engaging directly with some of the 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. This is especially the case with organisations that have not differentiated their answers between their systems; those responses that look a little optimistic with respect

to vulnerabilities; and those that have based answers on perceptions rather than logs / real data.

- Developing a nationally led programme of testing and exercising beginning with the most critical systems. This could include carefully controlled penetration testing on reference and production systems.
- Revisiting the national picture on cyber skills, awareness and training to assess the validity of the optimistic picture given by this initial survey. Grow a cadre of trusted advisors who can, on a 1-2-1 basis, work with organisations to help them complete future year NCRA's. Also use these skills (via training) to test knowledge of responses to phishing attacks, reviews of secure configurations, and understanding of cyber issues.
- Prioritising working with the Aviation, Education, Healthcare, Private (Organisation) and Energy sectors to improve their access to, and use of, relevant threat intelligence.
- Conducting the NCRA annually and should work to have more organisations and sectors participate in the NCRA, to ensure a truer national picture of risks and impact to CII in Zambia and ensure CII improved security.
- For organisations with high impacts, determining whether they are all using similar technologies/manufacturers that could lead to multiple simultaneous system failures in many organisations from a particular cyber-attack vector.
- Checking the sectors that have a lower number of system than expected, to determine the overall participation rate and ensure all necessary organisations commit to future NCRA processes. It is also necessary to check that the systems recorded are the most critical.

Appendices

Appendix A: List of Abbreviations

ZICTA: Zambia Information and Communication Technology Authority

CII: Critical Information Infrastructure

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

NCRA: National Cyber Risk Assessment

Head Office

Stand No. 4909, Corner of Independence
and United Nations Avenues
P.O. Box 36871, Lusaka—Zambia
info@zicta.zm, www.zicta.zm
Toll Free: 7070
Tel: +260 211 378200

Copperbelt

Plot 2735, Liberia Road
Trade Fair Grounds
Ndola—Zambia
Tel: +260 212 651032

Muchinga

Plot 888, Nkakula Street
Chinsali—Zambia
Tel: +260 211 378244

Southern

No. 626-8, Unit G.03
Butala House
Pioneer Street
Choma—Zambia
Tel: +260 211 000000

Eastern

Plot No. 56, Bishop John Osmer's
Office Complex, Church Road
Chipata—Zambia
Tel: +260 211 378246



ZICTA

A Regulator at the Nexus
of an Inclusive Digital Economy