

Ransomware: A Cyber Security Policy Brief

1st Kelvin Popovic
B.Sc Hons (IT & CS)
North-West University
kelvin.popovic@gmail.com

2nd Joshua Esterhuizen
B.Sc Hons (IT & CS)
North-West University
joshua.esterhuizen27.com

3rd Jumanah Al-Hazba
B.Sc Hons (IT & CS)
North-West University
jumanah1997@gmail.com

4th Affaan Muhammad
B.Sc Hons (IT & CS)
North-West University
affaanm94@gmail.com

Abstract—This document is a model and instructions for L^AT_EX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. ***CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

Index Terms—component, formatting, style, styling, insert

and inconvenient to attack due to faster and more appropriate reactions.

I. INTRODUCTION

As part of the Cyber 9/12 Strategy Challenge: South Africa Regional Competition in 2021, this brief focuses on recommendations for actors to follow, both non-state and state. It discusses the long and short impacts of these recommendations as well as which agencies are responsible for these recommendations. Furthermore, this policy will discuss whether an actor should attribute the threat and how to respond to these Ransomware threats.

II. LONG AND SHORT TERM IMPACT OF THE RECOMMENDATIONS

A. Short term impact

The short term impact of implementing the recommendations will be:

The high initial cost to implement the policy and provide appropriate training to employees and users that will ultimately remedy any further significant costs from incidents and reputation loss as a result. The short term impact will also enable the organisation to create a clear and comprehensive incident response plan and backups to recover if any further attacks are initiated. The inclusion of a report plan lets users and employees know exactly how and where to report suspicious activity that technicians can assess faster. Immediately removing/disconnecting the affected system to prevent the attack from propagating within the system will significantly improve the short term outcome. The restructuring of access to a least-privilege principle and segmentation of the network will make internal and external systems more inconvenient to compromise as a whole.

B. Long term impact

The long term impact of the recommendations will, over time, affect the organisational culture surrounding security and the responses to security violations. The shared goals of improving security in the organisation will vastly enhance the identification of attacks, responses, and restoration of systems and reporting incidents. The long term impact from additional security and response will make the system more resilient