Cyber Resilience

Protecting your most valuable asset!

|  |  |  |
| --- | --- | --- |
| **First Author** | **Second Author** | **Third Author** |
| *Greg Hewitson**UK**Greg\_Hewitson@Dell.com* | ***TBA****Country**first.author@email.edu**ORCID* | ***TBA****Country**first.author@email.edu**ORCID* |
|  |  |  |

# Introduction (***cyber Resilience***)

## Data that is at the heart of ransomware attack. Thanks to the rapid digital transformation happening today, data has become an organization’s most critical asset.

## Attackers know this very well and target their attack to gain access to your critical data.

## When they have access to your data, attackers can do multiple things. They can remove access to your own data by encrypting the contents with a key. They also attack data protection techniques to make sure that all restore capabilities are deleted. This way they increase the probability that you’ll pay for the for the key to unlock your data again. This is known as an encrypting ransomware attack. If the value of the content is high, they can also ask to pay a ransom to prevent this content from being shared. OR they can use this information for espionage and try to remain in stealth modus as long as possible (like SolarWinds attack)

 BUT NOT ALL DATA IS EQUAL!

# Description

## What is Cyber Resilience and what’s best practice. Here we’ll take a deeper dive at the bigger picture.

## Cyber Resiliency = The capacity for an organisation to protect, detect, respond to and recover from a cyber-attack with minimal impact. It’s clear that every organization will have a different cyber resilience strategy, which makes creating a cyber resiliency strategy not an easy task. Different frameworks have been created to guide organizations in building their own cyber resiliency strategy.

## We like to utilize the Cyber Security Framework (CSF) from the National Institute of Standards and Technology (NIST). This framework can help to create a common language between the board of directors, your IT administrators, your partners, and your customers during the complex task of creating and maintaining a cyber resiliency strategy. The NIST CSF consists of 5 pillars for 5 core functions of the framework:

## Identify: understand what you have in your organization and assess the risk. Define a target security profile of your organization.

## Protect: how are you going to defend what you have against the known bad

## Detect: detect suspicious behavior, infiltrations, and breaches

## Respond: how to respond when a detection is made?

## Recovery: how to get your business back up and running.

## Every organization should identify its target profile by going through the list of security controls and identifying

## We’ll then take the audience through how to understand their current security profile and what their target security profile steps are to mitigate Cyber threats to their critical assets.

# TARGET AUDIENCE

## This topic is best suited to C-Suite level, IT Storage managers and data preservation officers.

# REFERENCES

## **University of Texas at San Antonio**

## Written story: https://www.delltechnologies.com/asset/en-us/products/storage/customer-stories-case-studies/delltechnologies-customer-story-the-university-of-texas-san-antonio.pdf

## [Video Testimonial](https://www.delltechnologies.com/en-us/video-collateral/h18929-cv-powerscale-u-of-texas-san-antonio.htm): https://www.delltechnologies.com/en-us/video-collateral/h18929-cv-powerscale-u-of-texas-san-antonio.htm

## [Short Social Video](https://www.delltechnologies.com/en-us/video-collateral/h18930-cv-powerscale-u-of-texas-san-antonio-quotes.htm): https://www.delltechnologies.com/en-us/video-collateral/h18930-cv-powerscale-u-of-texas-san-antonio-quotes.htm

## [Perspectives Customer Story (Kendra Ketchum)](https://www.delltechnologies.com/en-us/perspectives/how-wartime-medic-kendra-ketchum-became-a-tech-trailblazer/): <https://www.delltechnologies.com/en-us/perspectives/how-wartime-medic-kendra-ketchum-became-a-tech-trailblazer/>

## PowerProtect Cyber Recovery for Sheltered Harbor, written story: https://www.dell.com/en-uk/dt/data-protection/cyber-recovery-solution.htm#tab0=0&pdf-overlay=//www.delltechnologies.com/asset/en-uk/products/data-protection/briefs-summaries/powerprotect-cyber-recovery-for-sheltered-harbor-solution-brief-h18199.pdf