A picture containing text

Description automatically generated

# Overview

IBM is pleased to present CUSTOMER\_NAME a report based on our findings from the IBM® Storage Cyber Resiliency Assessment which was completed by the CUSTOMER\_NAME Storage team in PRESENTATION\_DATE. It is understood that an effective cybersecurity resiliency program must be grounded in effective systems and processes that provide valuable insight into information and events that occur within an environment and provide the confidence for an orchestrated storage resiliency process in order to not disrupt CUSTOMER\_NAME’s business continuity objectives. By evaluating the current cybersecurity and resiliency environment, the organization now has specific recommendations designed to help increase the value of the solutions and services in its environment to meet RTO and RPO requirements.

Additionally, CUSTOMER\_NAME technology will be able to help deliver faster return on investment and higher operational productivity by leveraging time-tested practices and updates to product features and resiliency functions. It will be able to help decrease errors and inconsistency through the implementation of the incremental recommendations we have provided in this document.

# Executive summary

Based on the information gathered during our initial reviews within IBM as well as the responses on the assessment, CUSTOMER\_NAME has realized great value from its investment in cyber resilience and is generally above the average with other customers that IBM has worked with. However, there are a few areas where CUSTOMER\_NAME has exposure to risk resulting in unrecoverable data loss or corruption and where more value can be realized.

It is Important that CUSTOMER\_NAME’s senior management must understand that risk is the new normal. Being a digital enterprise in 2021 incurs significant risk and Cyber Resiliency (protection, data vaulting, air-gapping, and recovery) is now an absolute part of the cost of doing business.

We believe CUSTOMER\_NAME would benefit from a "customized refresher BCDR workshop" or round table discussion rather than a "building from a ground up" workshop considering there already is a good amount of implementation in place with disaster recovery and security. At a high level, there seems to be a disconnect from their end users’ expectations (unrealistic) and what's being provided (realistic). Revising documentation and solidifying SLAs on a per-system/application basis should be able to resolve a majority of this.

Cyber resiliency should be viewed as a dynamic and ever-evolving practice that requires continuous improvement and focus. With the continued expansion of the threat landscape and pace of technology change, it is imperative that organizations constantly take inventory of how they are doing and where they need to be evolving.

Please review the Recommendation Section for our roadmap, which, if followed, will improve functionality and increase the value realized from implementing resiliency and disaster recovery best practices and solutions. Establishing a mature cyber security and resiliency plan will enable a more proactive approach in detecting, identifying, and protecting their environments, as well as their ability to respond and recover quickly and effectively.

# Assessment Background Information

**Reference**

This assessment was based on the NIST Cyber Security Framework (CSF) and is focused on storage and the storage environment. Contains references to other industry recognized standards & frameworks: ISO, COBIT, ISA, Council on Cyber Security, among others.

A close up of a sign

Description automatically generated

**Purpose**

The Storage CR Assessment provides a bridge mechanism to assess client’s current state and identify gaps against best practice requirements based on the NIST CSF. It helps in the Identification of blind-spots and recommended areas for improvement.

**Maturity Level Definitions**

The numbers in the boxes will be referenced throughout this document to match the score with the maturity level.

A screenshot of a cell phone

Description automatically generated

# Value summary dashboard

**Executive Summary – Summary View**

The numbers in the table reference the current overall maturity level on each of the assessment’s categories.

**TOTAL\_SCORE\_REPLACE**

|  |  |  |
| --- | --- | --- |
|  | **Your score** | **Maturity Level** |
| **Total score** | **8.56** | **Mature** |
|  |  |  |
| **Identify** | **10.00** | **Leading** |
| Asset Management | 10.00 | Leading |
| Business Environment | 10.00 | Leading |
| Governance | 10.00 | Leading |
| Risk Assessment | 10.00 | Leading |
| Risk Management Strategy | 10.00 | Leading |
|  |  |  |
| **Protect** | **5.62** | **Developing** |
| Identity Management, Authentication and Access Control | 0.00 | Initial |
| Awareness Training | 10.00 | Leading |
| Data Security / Protective Technology | 5.21 | Developing |
| Information Protection Processes and Procedures | 10.00 | Leading |
| Maintenance | 10.00 | Leading |
|  |  |  |
| **Detect** | **7.17** | **Practicing** |
| Anomalies and Events | 8.65 | Mature |
| Security Continuous Monitoring | 5.58 | Developing |
| Detection Processes | 7.33 | Practicing |
|  |  |  |
| **Respond** | **10.00** | **Leading** |
| Response Planning | 10.00 | Leading |
| Response Communications | 10.00 | Leading |
| Analysis | 10.00 | Leading |
| Mitigation | 10.00 | Leading |
| Improvements | 10.00 | Leading |
|  |  |  |
| **Recover** | **10.00** | **Leading** |
| Recovery | 10.00 | Leading |
| Recovery Planning | 10.00 | Leading |
| Recovery Improvements | 10.00 | Leading |
| Recovery Communications | 10.00 | Leading |
|  |  |  |
|  |  |  |

**Executive Summary – Maturity Level Graphics**

The spider charts in the table below reference the current overall maturity level scores on each of the assessment’s categories.

|  |
| --- |
| **MATURITY\_GRAPH\_1** |
| **MATURITY\_GRAPH\_2** |

**Executive Summary – Ransomware % Achieved**

The pie chart in the table below represents a percentage of ransomware related questions within the assessment which were answered with yes (1) and partially (.5) on the green area and with no (0) and partially (.5) on the red.

|  |
| --- |
| **RANDSOMWARE\_GRAPH** |

**Insights**

This chart shows 58% of ransomware readiness. This is evidence that CUSTOMER\_NAME has implemented resilient systems and procedures with the environment and is on a good track to protect the environment from and in case of a ransomware attack. The missing 42% shows a large area for improvements that can be beneficial for the team. At the moment, we don’t believe CUSTOMER\_NAME is well positioned to come back from a Ransomware attack. Consider fully implementing a physical, or logical air-gap as well as an immutability solution. Retention sets and isolated local vaults could make a big impact. A workshop and follow-up can be scheduled on that topic.

In terms of detection, we recommend keeping an eye and setting alert thresholds for virtual machine block change rate, compression and deduplication. Any sudden or larger than normal changes could be red flags and a warning that Ransomware is in the system and encrypting data.

Additionally, simple best practices can have a high impact on this score, preparing for and testing these recommendations is key. For example, during recovery we recommend “coming back” on a testing or sandbox environment before going to production. This will enable the company to ensure that the restore won’t cause follow on problems as well as make sure that the data is not compromised or corrupted.

Consider leveraging an incident response retainer with a security company. That way, if an incident occurs, you can give them a call and they will assist with the response in your environment. IBM does offer those services through IBM X-Force Red IRIS Team.

Lastly, we recommend reviewing, creating, and updating Response plans (Incident Response, Business Continuity, and Cyber Resiliency) and recovery plans (Incident Recovery and Disaster Recovery).

**Executive Summary – Percentage Achieved Per Category**

The graph in the table represents 14 categories that were measured by the assessment and CUSTOMER\_NAME’s percentage of each category achieved.

|  |
| --- |
| **EXECUTIVE\_GRAPH** |

**Insights**

CUSTOMER\_NAME has proven to have great understanding of their systems and procedures, as evidenced by their diligent practices around documentation, infrastructure, and personnel training. The Storage team at CUSTOMER\_NAME has proven to apply lessons learned and are proactively looking for ways to improve.

ISSUE\_1

ISSUE\_2

ISSUE\_3

ISSUE\_4

Implementing simple best practices and having deeper conversations in specific areas can lead to higher scores.

# Recommended Initiatives

Table 1 highlights a prioritized list of major projects that IBM recommends be done to increase the value of the solution to your environment. Any or all these items may be addressed as per the risk appetite and budgetary constraints.

Table 2 highlights a prioritized list of minor projects that IBM recommends be done to increase the value of the solution to your environment. This list includes projects that the client is currently participating in but could use some enhancements. Any or all these items may be addressed as per the risk appetite and budgetary constraints.

|  |  |
| --- | --- |
| **Importance** | **Major Recommendations** |

Table - List of **Major** Initiatives

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 2 - Prioritized List of **Minor** Initiatives

|  |  |
| --- | --- |
| **Importance** | **Minor Recommendations** |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# *Summary*

CUSTOMER\_NAME’s current cyber resiliency posture with an overall score of 6.40 is slightly below average when compared with other organizations supported by IBM in their industry.

It is clear that CUSTOMER\_NAME has invested heavily in their security strategy, processes, and tools. CUSTOMER\_NAME should continue to integrate more tightly, the Disaster recovery, Business Continuity, Governance, and Security functions to encourage collaboration.

CUSTOMER\_NAME’s goal is to refresh their 10-year-old DR plans for latest cyber resiliency best practices. Based on our findings and their goals, CUSTOMER\_NAME would benefit from a series of disaster recovery refresher workshops or simply informal round table discussions segmented up to tackle a group of items rather than everything at once. CUSTOMER\_NAME has both Z and distributed environments. The Z environment leverages VTL, GDPS, and appears to be a bit more squared away than open, probably due to the standardized methodology of the Z platform. We recommend the Z teams leverage the cyber resiliency workshops specialized for System Z to maximize the use of their time.

The team members participating in the assessment were primarily storage/disaster recovery focused. There are teams/departments that specialize in security, incident response and risk assessments, but may not be in full sync with systems/application owners and storage teams. It's quite common to find larger organizations with some level of disconnect especially during times of rapidly evolving standards. Due to the lack of information from external teams we will lean towards a more encompassing approach out of caution. We also recommend that the teams leverage this assessment and it’s finding to connect and update each other on their priorities and current practices.

For the distributed systems we can wrap multiple workshops around the following items of interest - not in any particular order:  
+ Update/Identify roles and responsibilities. (who does what during certain major events, i.e. during ransomware attack, site disaster, DDoS)  
+ Work with application/system owners to review/update/evaluate dependencies (verify data is classified appropriately, DR protections in place, and their SLA/RTO/RPO expectations are realistic)  
+ Review current environment in more depth, see if there are features or tools that can be leveraged to cover gaps or increase efficiency (i.e Splunk add-on, volume protection, dual admin control, insights alert conditions)  
+ Air Gap Workshop (covers logical, immutable, and physical)  
+ Round table discussion covering specifically cyber-attacks/rapid malware propagation, draft action item goal to build template sandbox/test environment for the purpose of mass restore exercises  
+ Backup environment sizing study

Additional workshops can be planned out based on CUSTOMER\_NAME’s interests and our recommendations.

Additionally, we recommend implementing the different best practice recommendations highlighted on the Major and Minor Recommendation Tables in order of importance.

Of course, IBM would like to be CUSTOMER\_NAME’s partner and assist with the journey to a more resilient environment.

# References

1. *Verizon -* [*2019 Data Breach Investigations Report*](https://enterprise.verizon.com/resources/reports/dbir/)
2. *Ponemon Institute –* [*The Evolving Role of CISOs and their Importance to the Business*](https://f5.com/Portals/1/PDF/labs/Evolving_Role_of_CISOs_Aug2017.pdf?ver=2017-09-18-100218-007)
3. *NIST -* [*NIST Cybersecurity Framework*](https://www.nist.gov/cyberframework)
4. *Harvard Business School -* [*Six Sigma Meets the Service Economy - Six Sigma: It's Not Just for Manufacturing*](https://hbswk.hbs.edu/archive/six-sigma-meets-the-service-economy-six-sigma-it-s-not-just-for-manufacturing)
5. *Security Intelligence –* [*What is Threat Modeling and How does it Impact Application Security*](https://securityintelligence.com/posts/what-is-threat-modeling-and-how-does-it-impact-application-security/)
6. *IOT for All -* [*The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History*](https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/)
7. *NIST -* [*Developing Cyber Resilient Systems: A Systems Security Engineering Approach*](https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final)
8. *IBM Red Hat -* [*What is DevSecOps?*](https://www.redhat.com/en/topics/devops/what-is-devsecops)
9. *CSO Online -* [*Will your backups protect you against ransomware?*](https://www.csoonline.com/article/3075385/will-your-backups-protect-you-against-ransomware.html)
10. *Security Exchange Commission -* [*Guidance on Public Company Cybersecurity Disclosures*](https://www.sec.gov/rules/interp/2018/33-10459.pdf)
11. *Harvard Business School –* [*CFOs Don’t Worry Enough About Cyber Risk*](https://hbr.org/2017/12/cfos-dont-worry-enough-about-cyber-risk)

© Copyright IBM Corporation 2021

IBM Corporation New Orchard Road Armonk, NY 10504

Produced in the United States of America PRESENTATION\_DATE

IBM, the IBM logo, ibm.com, QRadar, and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Microsoft and Active Directory are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS

FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION

OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result

in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

--- This page has been intentionally left blank ---