

**{Response.BusinessName}**

****

CyberSecurity Assessment

Dear {Response.FirstName},

Thank you for completing this sample CyberSecurity Assessment. This report is just an example of what Brilliant Assessments can produce.

As a user of Brilliant Assessments, you would normally copy this report text onto your own letterhead and then start modifying it to reflect your brand and market positioning.

There are lots of different options for merging in data and graphs from the software, but the most flexible part is the layout of this report – being a word document – you are really quite unlimited as to what you can do!

Please note that the template assessment is provided as a starting point and no claim is made as to its suitability as a cybersecurity assessment. We hope though, that it saves you time in building your own!

# YouR overall Cybersecurity Rating

|  |  |
| --- | --- |
| {Gauge[Survey Height=200]} | Your overall rating score is {RatingScore.Score}.Maturity Levels are allocated from 0 (zero) to 4. Maturity Level 3 is considered adequate for most commercial organizations. Maturity Level 4 is recommended for high risk environments. You are: {Rating.RatingText} |

# Assessment Summary

## Managing Servers

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=2 Height=50]} |

## System Administrators

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=3 Height=50]} |

## Managing Workstations

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=4 Height=50]} |

## End Users

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=5 Height=50]} |

# Detailed Report

# Managing Servers

## Physical Security

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=2 SubSectionNo=1 Height=50]} |

The lowest level of cybersecurity is physical security; however, it is often overlooked.  Even easier than how hacking into your database may be, for example, the ability to pick up a backup copy of your system.  This requires a much lower level of technical expertise, bringing "ordinary" disgruntled or disengaged staff into your risk profile.

* {RatingSubsection.RatingText[SectionNo=2 SubSectionNo=1]}

## Server Operating System Patching

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=2 SubSectionNo=2 Height=50]} |

Applying patches for extreme security risk vulnerabilities in server operating systems ensures the most up to date protections against new and legacy threats.

* {RatingSubsection.RatingText[SectionNo=2 SubSectionNo=2]}

## Patching Applications on Servers

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=2 SubSectionNo=3 Height=50]} |

Applying patches for extreme security risk vulnerabilities in server-based applications like web server software, other server applications that store important (sensitive or high-availability) data, and all other internet-accessible server applications is critical to ensure the most up to date protection against new and legacy threats.

* {RatingSubsection.RatingText[SectionNo=2 SubSectionNo=3]}

## Backups

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=2 SubSectionNo=4 Height=50]} |

Backups of critical data and information are crucial for Incident Readiness and Incident Response. Taking, maintaining and testing backups helps your organization set a threshold for survivability after an incident that may compromise data.

* {RatingSubsection.RatingText[SectionNo=2 SubSectionNo=4]}

# System Administrators

## Administration Privileges

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=3 SubSectionNo=1 Height=50]} |

Administration passwords should have more rigorous rules applied to them because the consequences of breach are high.  Auto-generated passwords are generally more secure and harder to crack by brute force attacks than self-created passwords.

* {RatingSubsection.RatingText[SectionNo=3 SubSectionNo=1]}

## System Administrators Multi-Factor Authentication

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=3 SubSectionNo=2 Height=50]} |

Multifactor Authentication (MFA) is one of the best ways of protecting organizational data. Most data breaches occur through compromised authentication. Although strong passwords are crucial to protecting data, adding multifactor authentication adds a substantial layer of security to make your data safer.

Multifactor Authentication methods suitable for most environments are:

* Universal 2nd Factor (U2F) security keys (USB or NFC based)
* physical One Time Passcode (OTP) tokens.
* biometrics,
* smartcards.
* {RatingSubsection.RatingText[SectionNo=3 SubSectionNo=2]}

# Managing Workstations

## Workstation Operating System Patching

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=4 SubSectionNo=1 Height=50]} |

Reviewing vendor patches criticality and applicability helps your organization determine which order to patch applications in to protect your systems most effectively.

* {RatingSubsection.RatingText[SectionNo=4 SubSectionNo=1]}

## Workstation Application Patches

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=4 SubSectionNo=2 Height=50]} |

Applying patches for extreme security risk vulnerabilities in commonly used workstation applications ensures the most up to date protection against new and legacy threats.

Because of their high use, the following applications are often targeted:

* Adobe Flash
* Web browsers
* Microsoft Office
* Oracle Java
* PDF viewers
* {RatingSubsection.RatingText[SectionNo=4 SubSectionNo=2]}

## Application Whitelisting

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=4 SubSectionNo=3 Height=50]} |

Application whitelisting creates a "trusted" list of applications that have been thoroughly vetted by the organization, greatly reducing the chances for unstable, malicious or otherwise harmful applications to compromise organizational systems. With no defined and enforced list of trusted applications, the organization risks non-conformity, and therefore incompatibility in applications, and more importantly, risks unvetted applications compromising organizational systems.

* {RatingSubsection.RatingText[SectionNo=4 SubSectionNo=3]}

## User Application Hardening

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=4 SubSectionNo=4 Height=50]} |

There are basic tools any organization can use to make a breach by a variety of the most common cyber threats more difficult, and less likely. By applying some relatively simple application hardening measures, you give your organization an extra layer of protection against many common threats and vectors.  Typical hardening measures include removing unused software and functionality.

* {RatingSubsection.RatingText[SectionNo=4 SubSectionNo=4]}

## Microsoft Office Macros

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=4 SubSectionNo=5 Height=50]} |

Attackers like to target any weaknesses in the design of an application whenever possible. Using implementation bugs, such as ones that can be found through fuzzing, can be viable for an attacker. Securing and limiting the use of Microsoft Office Macros can help secure your organization with an easily fortified layer of security.

* {RatingSubsection.RatingText[SectionNo=4 SubSectionNo=5]}

# End Users

## End User Controls

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=5 SubSectionNo=1 Height=50]} |

Password complexity rules help keep user passwords safer from guessing or brute force attempts to hack.

* {RatingSubsection.RatingText[SectionNo=5 SubSectionNo=1]}

## User Multi-Factor Authentication

|  |  |
| --- | --- |
|  | {ProgressBar[SectionNo=5 SubSectionNo=2 Height=50]} |

Multifactor Authentication (MFA) is one of the best ways of protecting organizational data. Most data breaches occur through compromised authentication. Although strong passwords are crucial to protecting data, adding multifactor authentication can add a layer of security to make your data safer.

* {RatingSubsection.RatingText[SectionNo=5 SubSectionNo=2]}