CSC 10

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 10.0

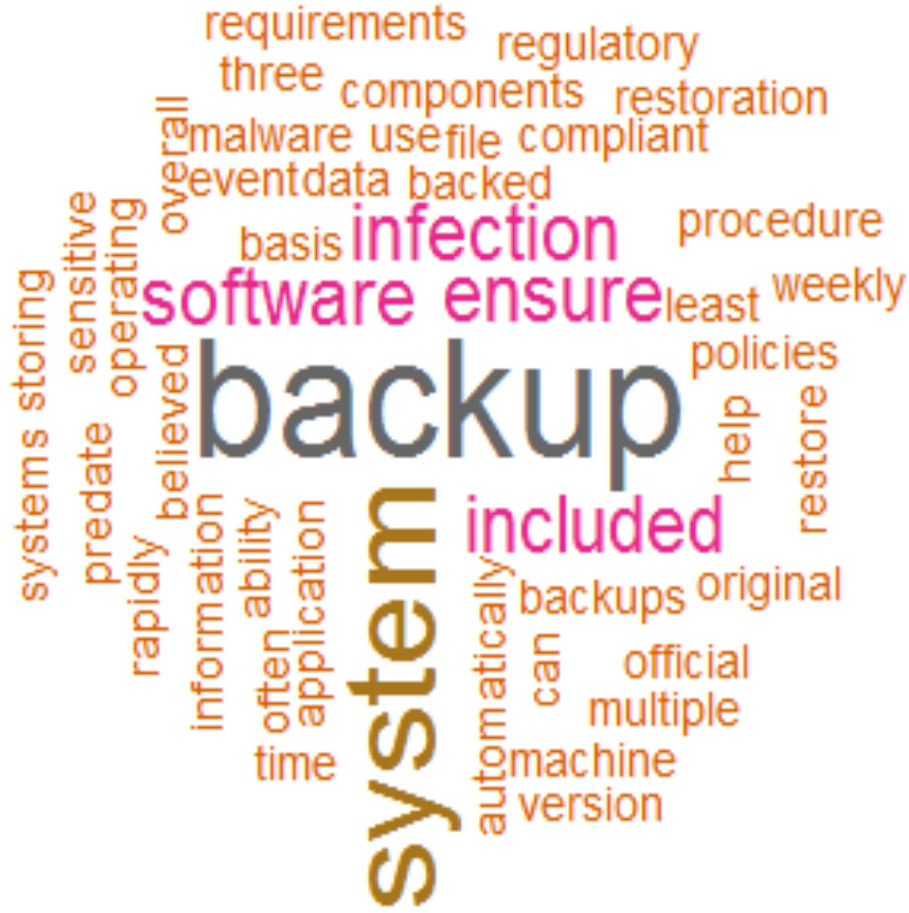
[1] "Critical Security Control #10: Data Recovery Capability"

[1]

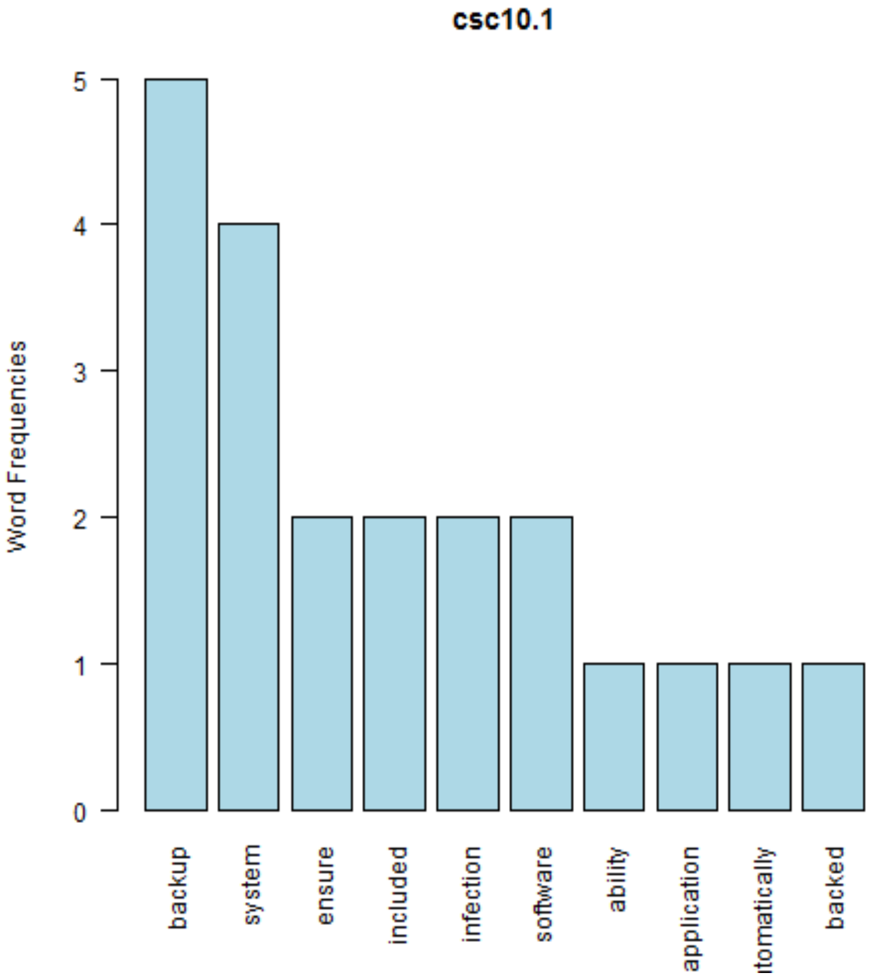
[1] [1] "To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Â Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security."

CSC 10.1

```
[1] “backup + system”
```



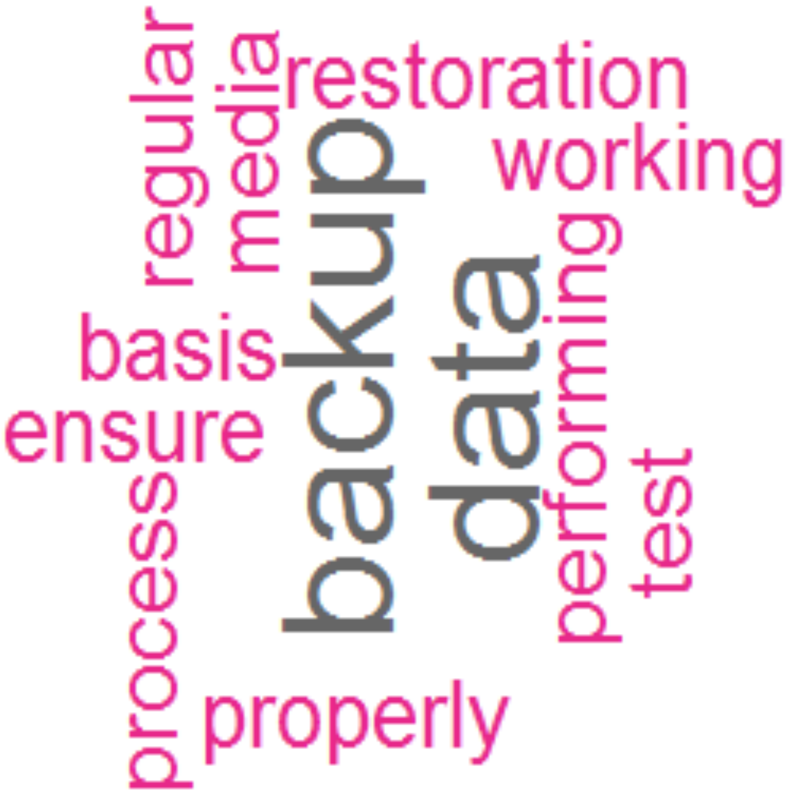
```
null device 1
```



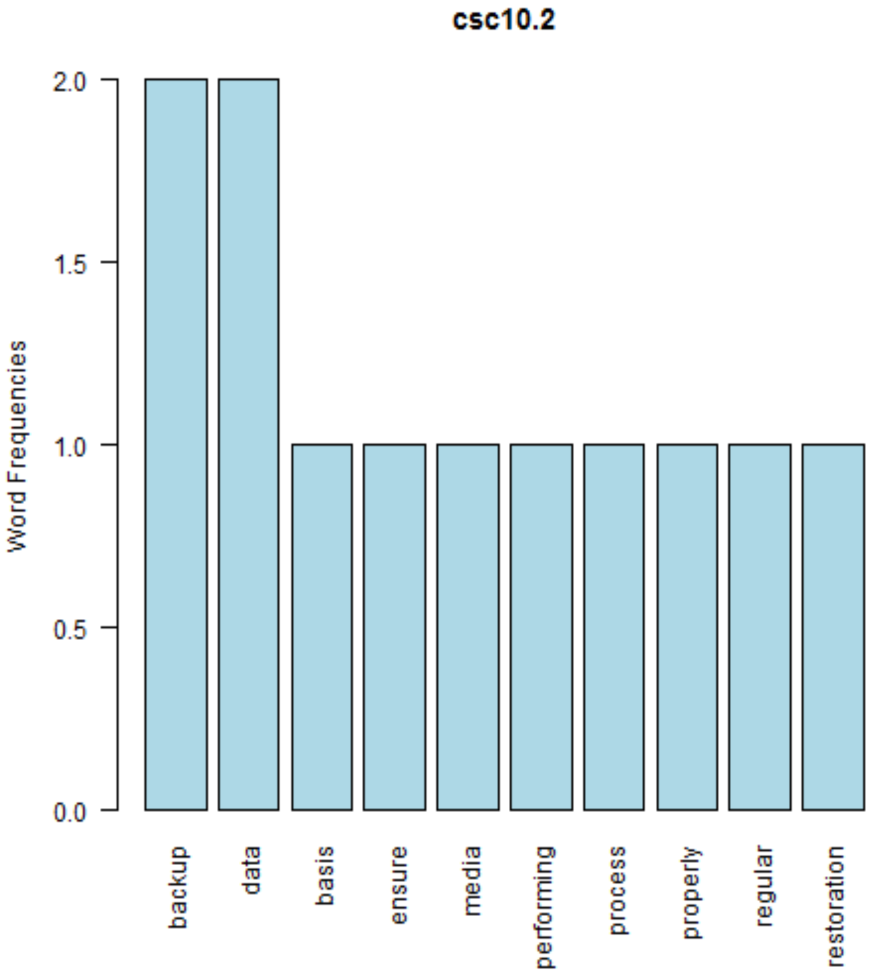
null device 1 [1] "Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements."

CSC 10.2

```
[1] “backup + data”
```



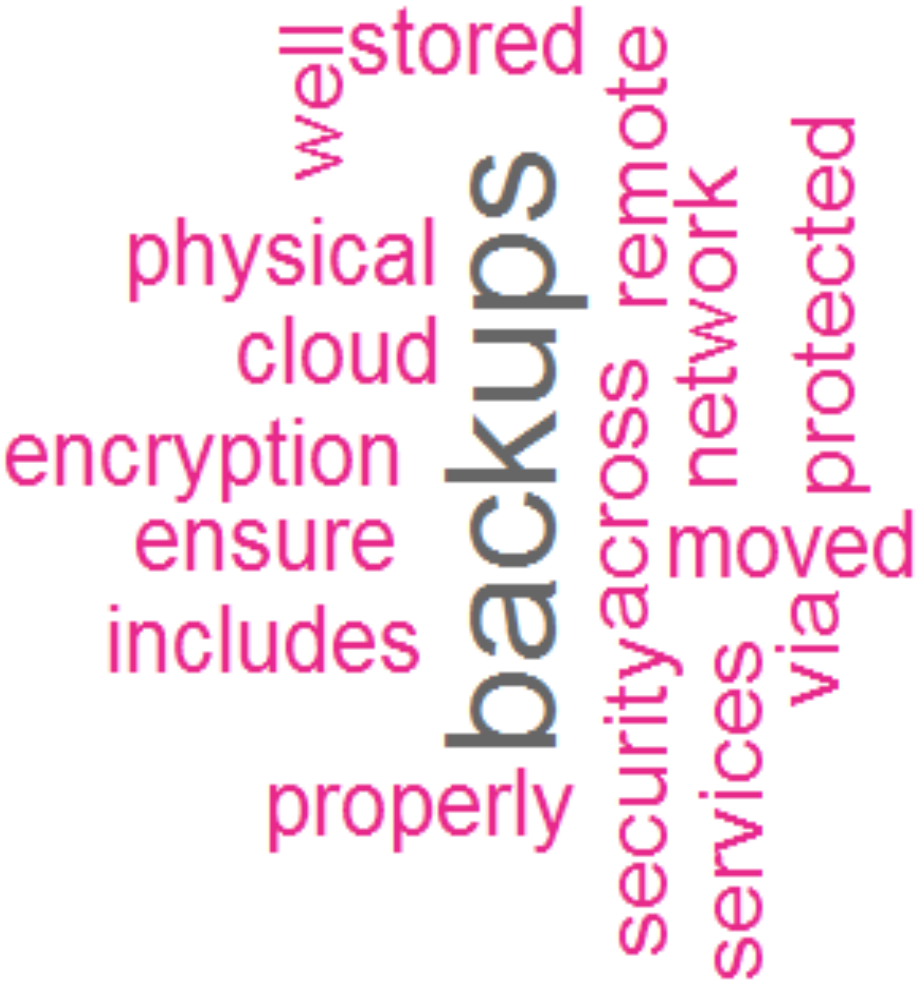
```
null device 1
```



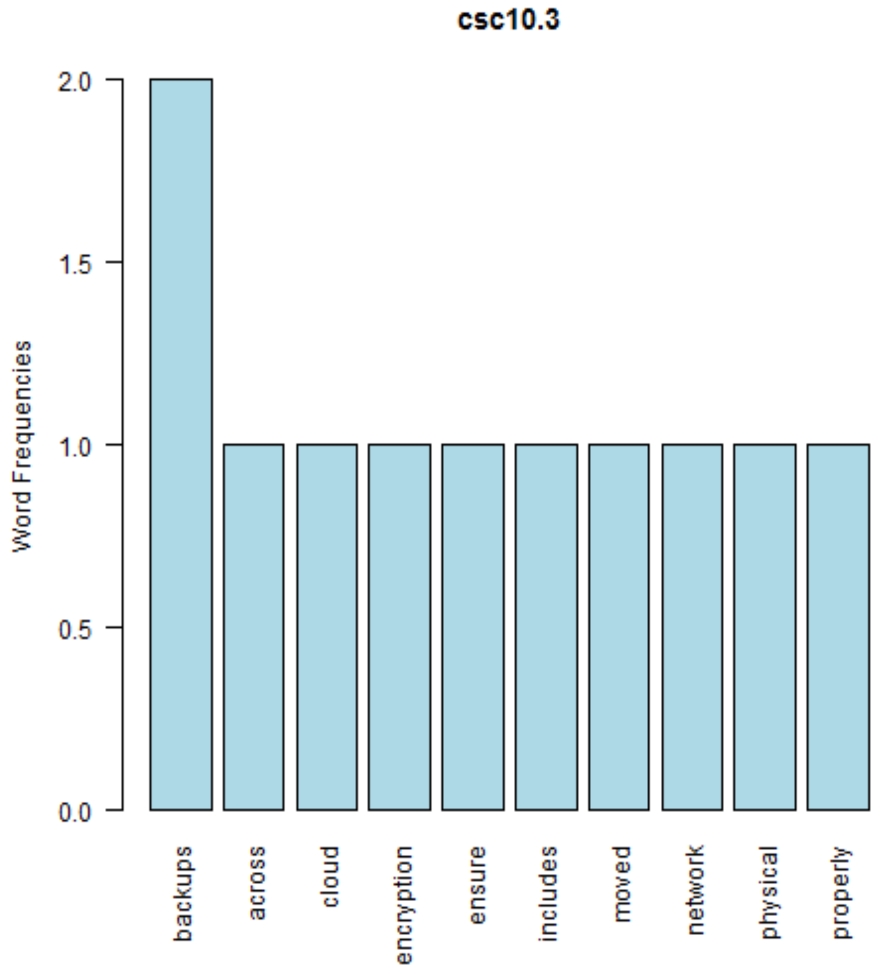
null device 1 [1] “Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.”

CSC 10.3

[1] “backups + across”



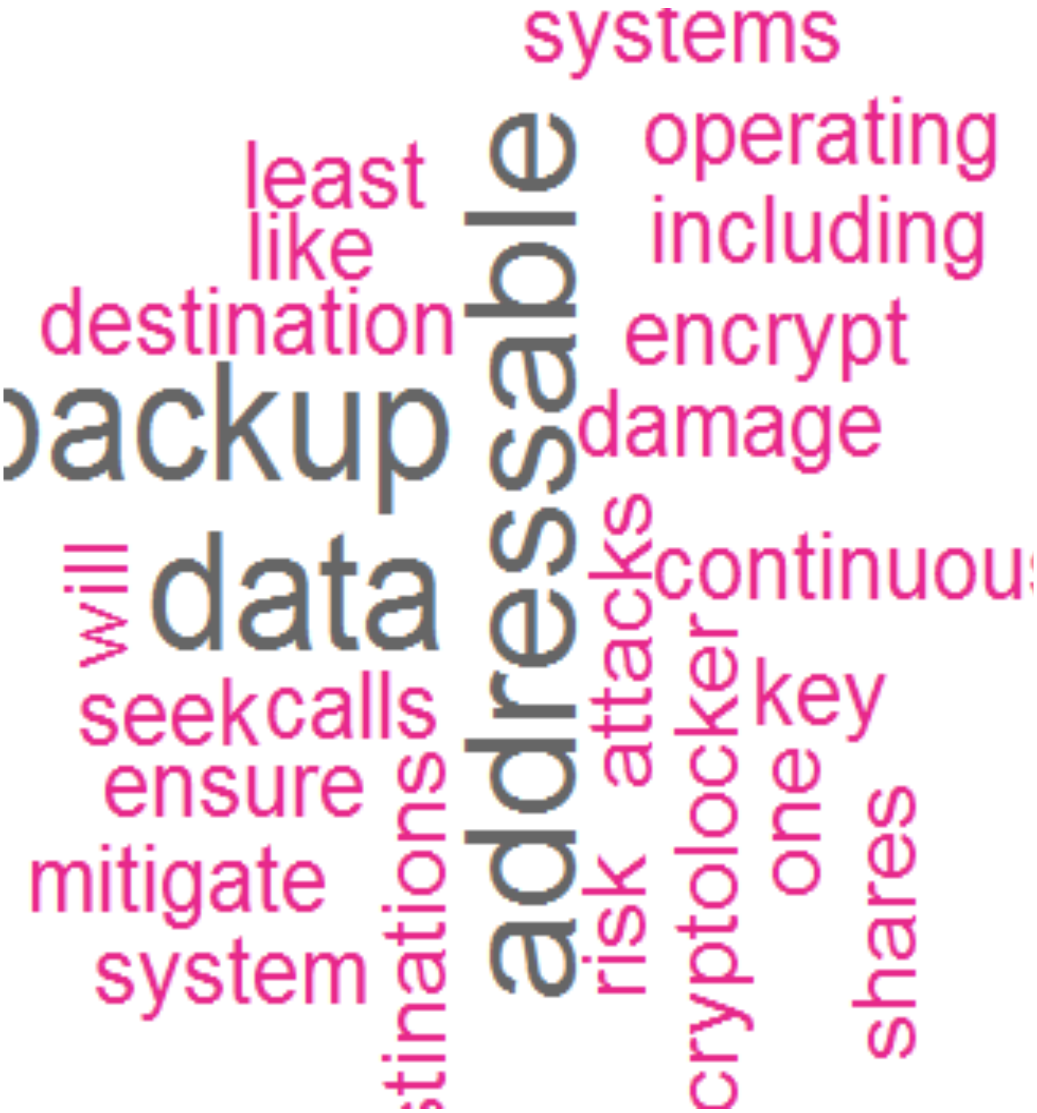
null device 1



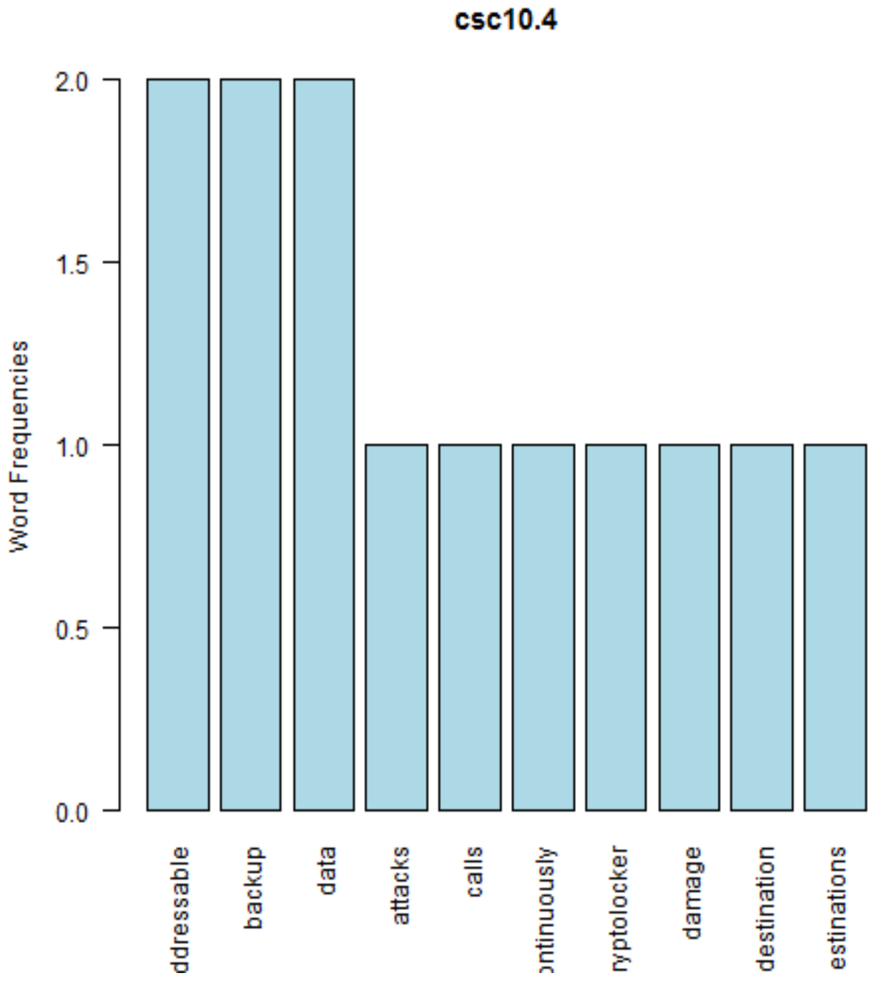
null device 1 [1] “Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.”

CSC 10.4

[1] “addressable + backup”



null device 1



null device 1 [1] “Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.”

[2]

[2] http://www.pandasecurity.com/mediacenter/malware/cryptolocker/