CSC 14

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 14.0

[1] "Critical Security Control #14: Controlled Access Based on the Need to Know"

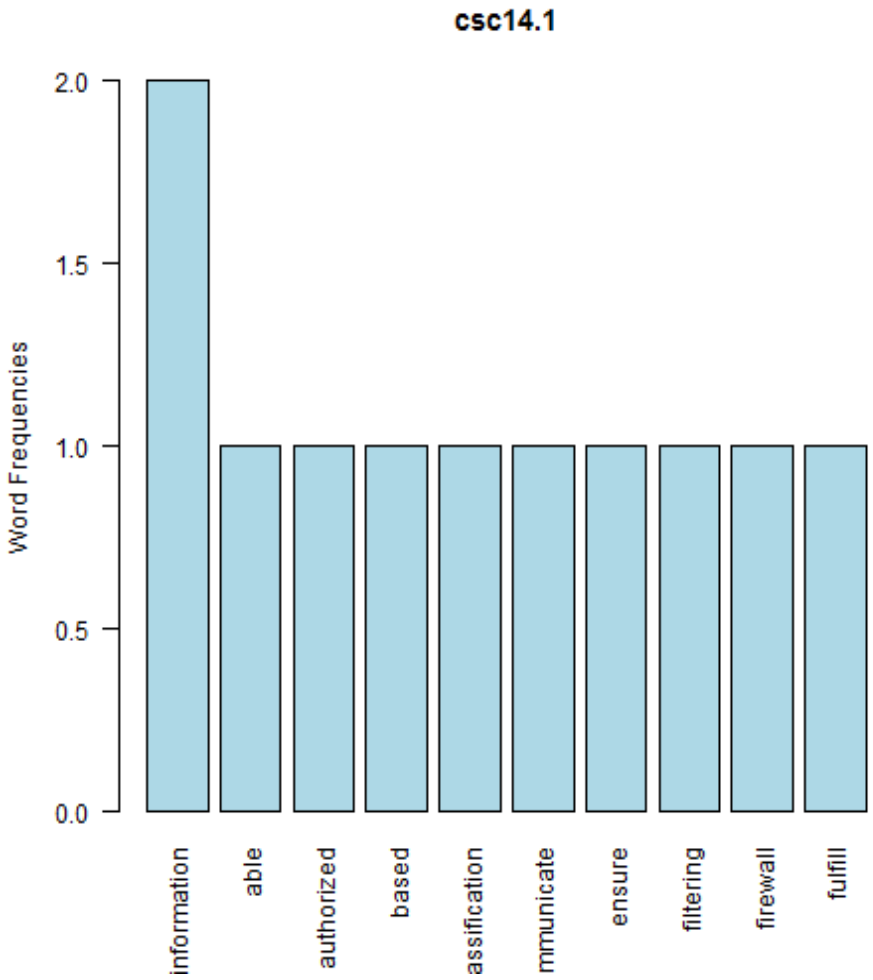
[1]

[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 14.1

[1] “information + able”

null device 1

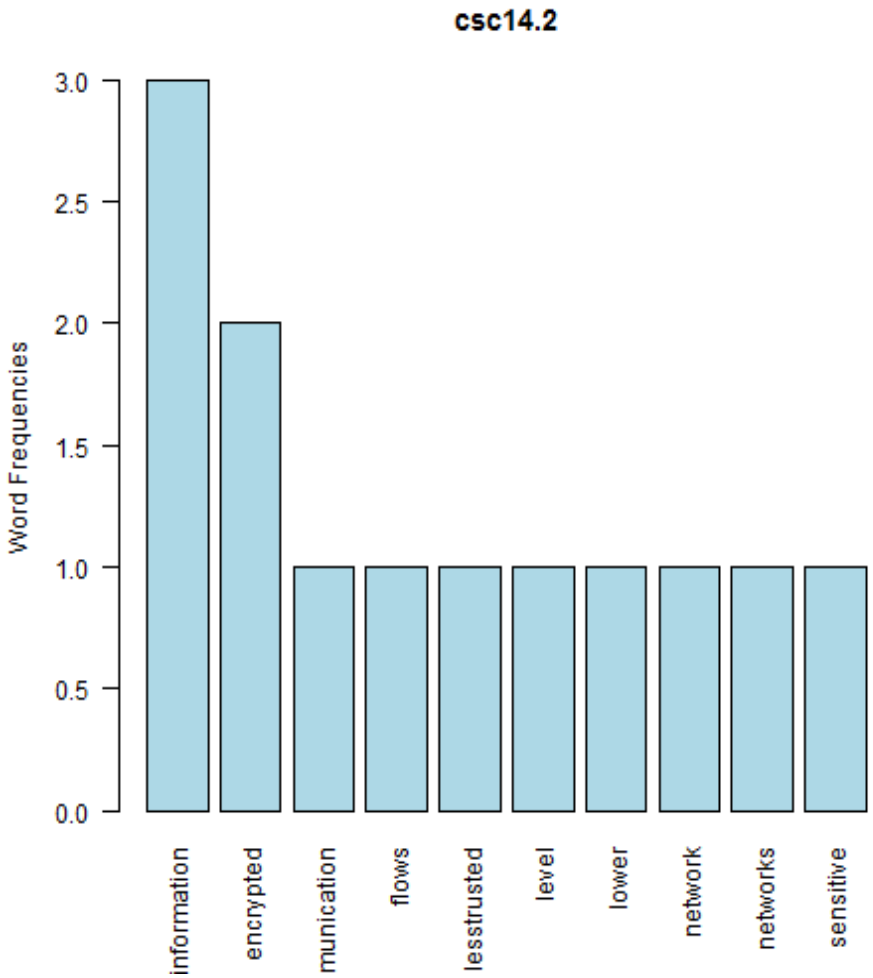


null device 1 [1] “Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.”

CSC 14.2

[1] “information + encrypted”

null device 1

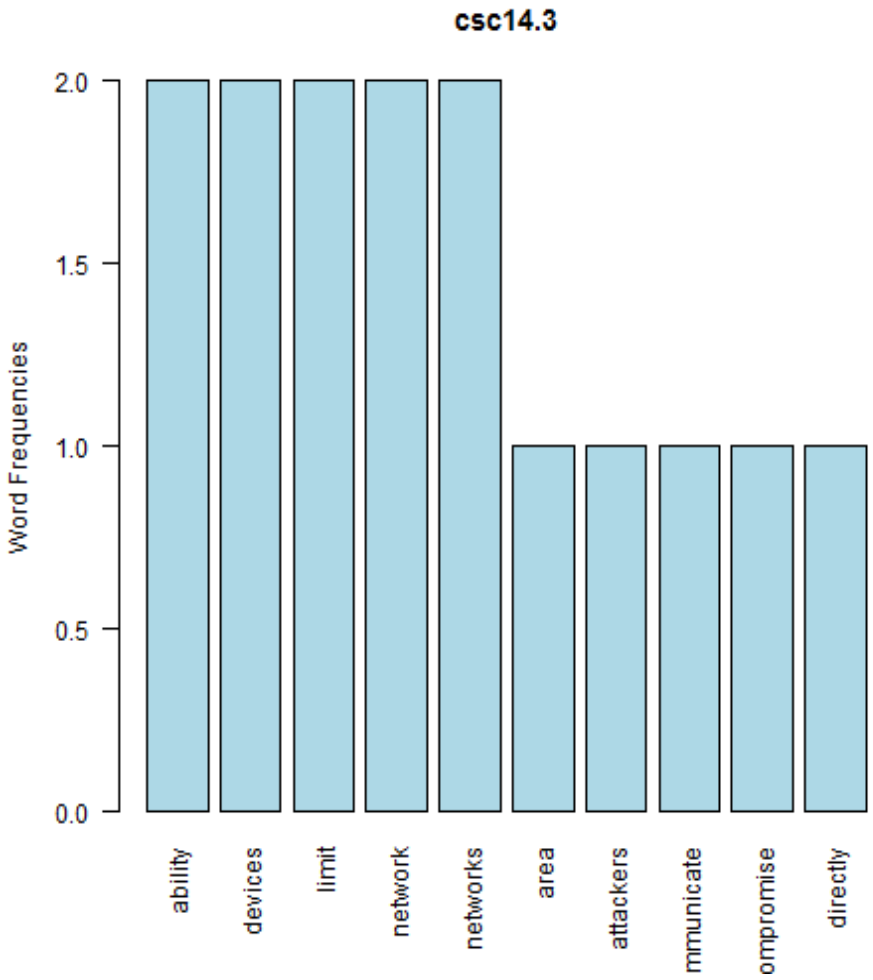


null device 1 [1] "All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted."

CSC 14.3

[1] “ability + devices”

null device 1

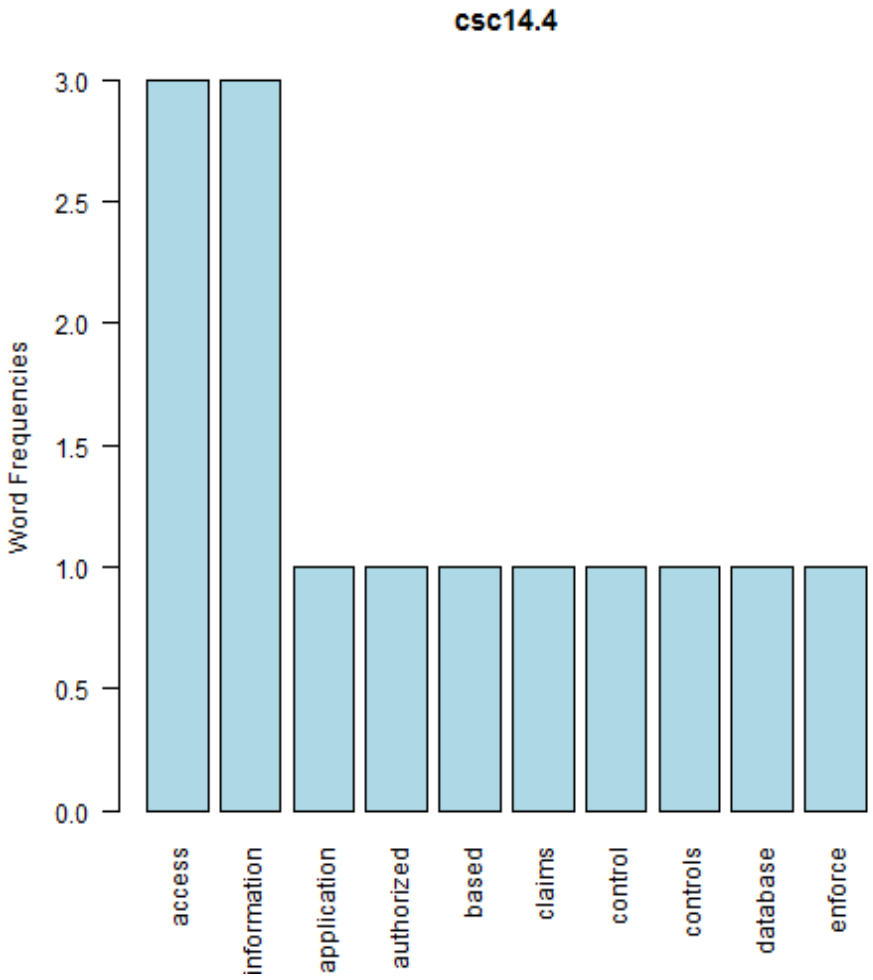


null device 1 [1] “All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.”

CSC 14.4

[1] "access + information"

null device 1

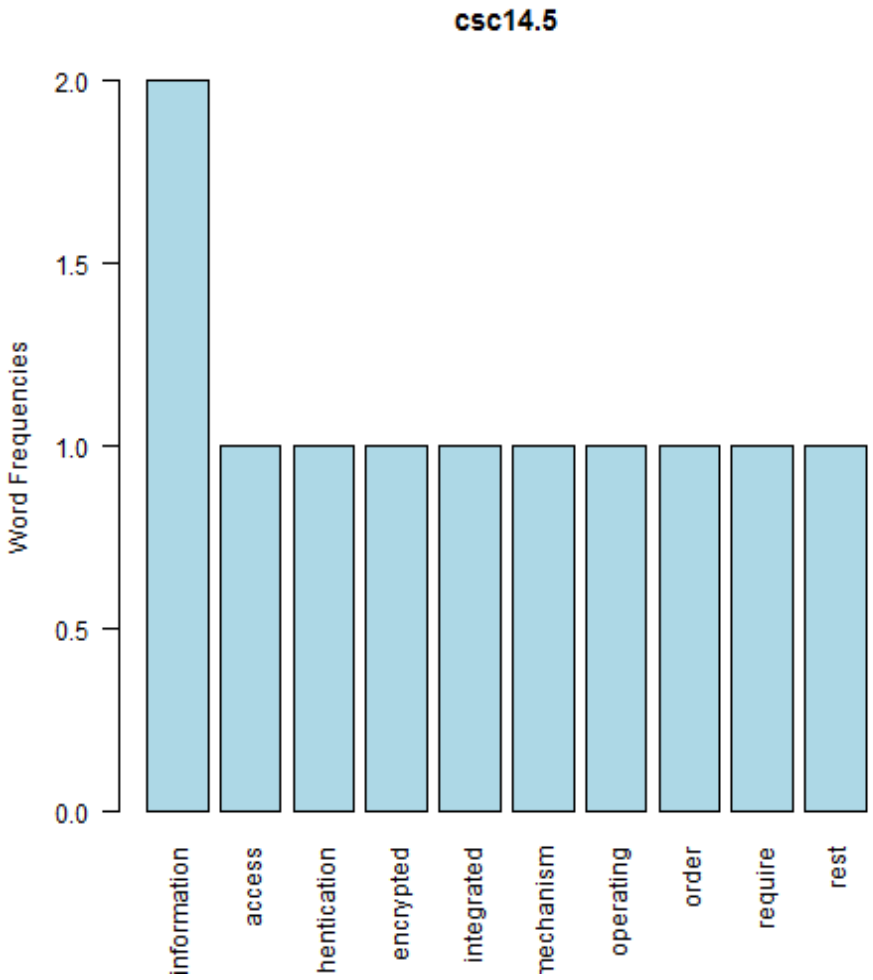


null device 1 [1] "All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities."

CSC 14.5

[1] “information + access”

null device 1

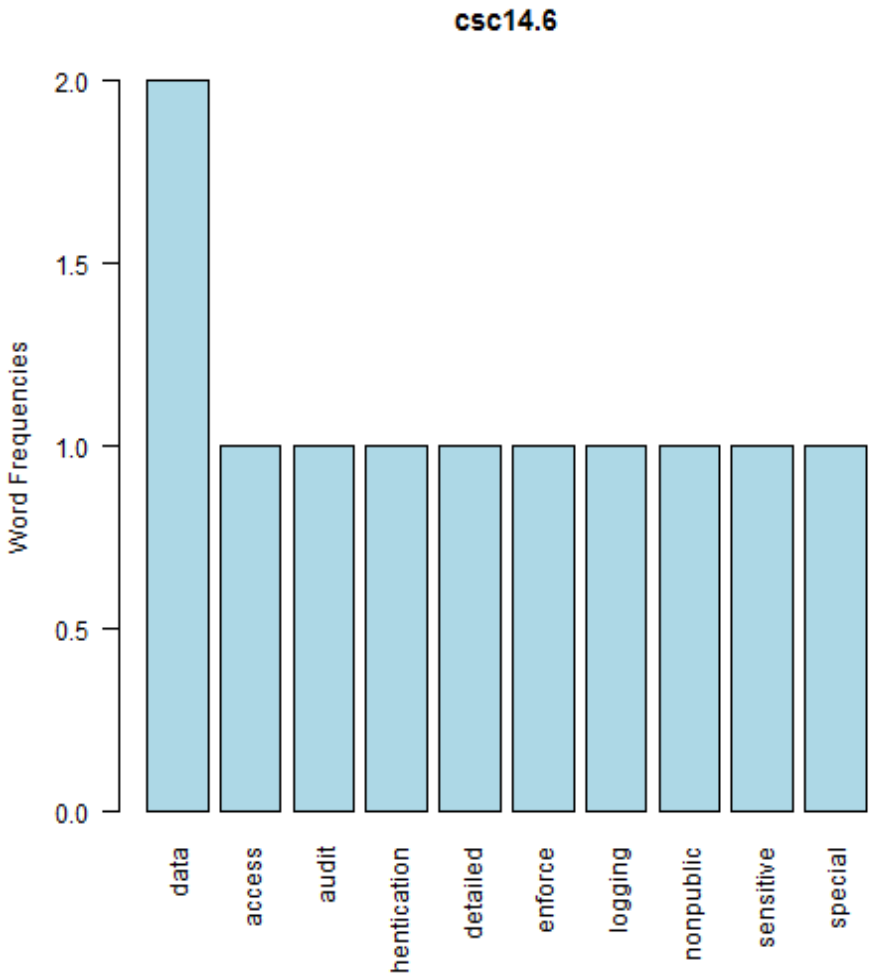


null device 1 [1] “Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.”

CSC 14.6

[1] “data + access”

null device 1

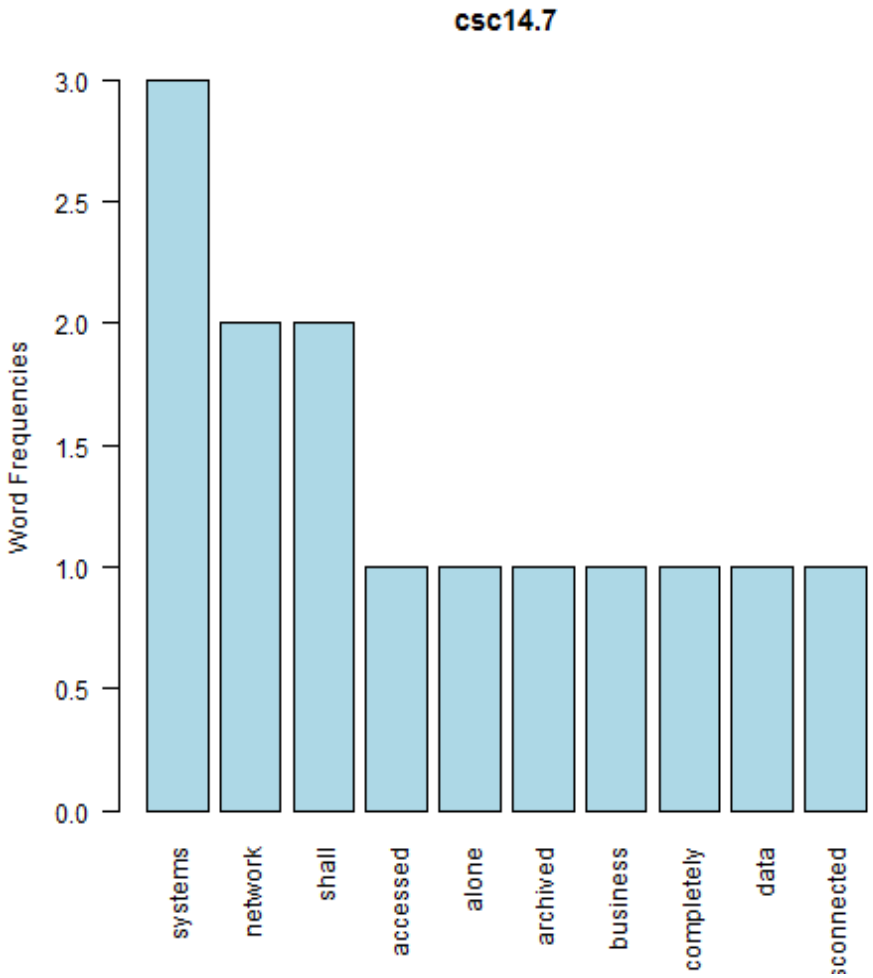


null device 1 [1] “Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.”

CSC 14.7

[1] “systems + network”

null device 1



null device 1 [1] "Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed."