CSC 19

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 19.0

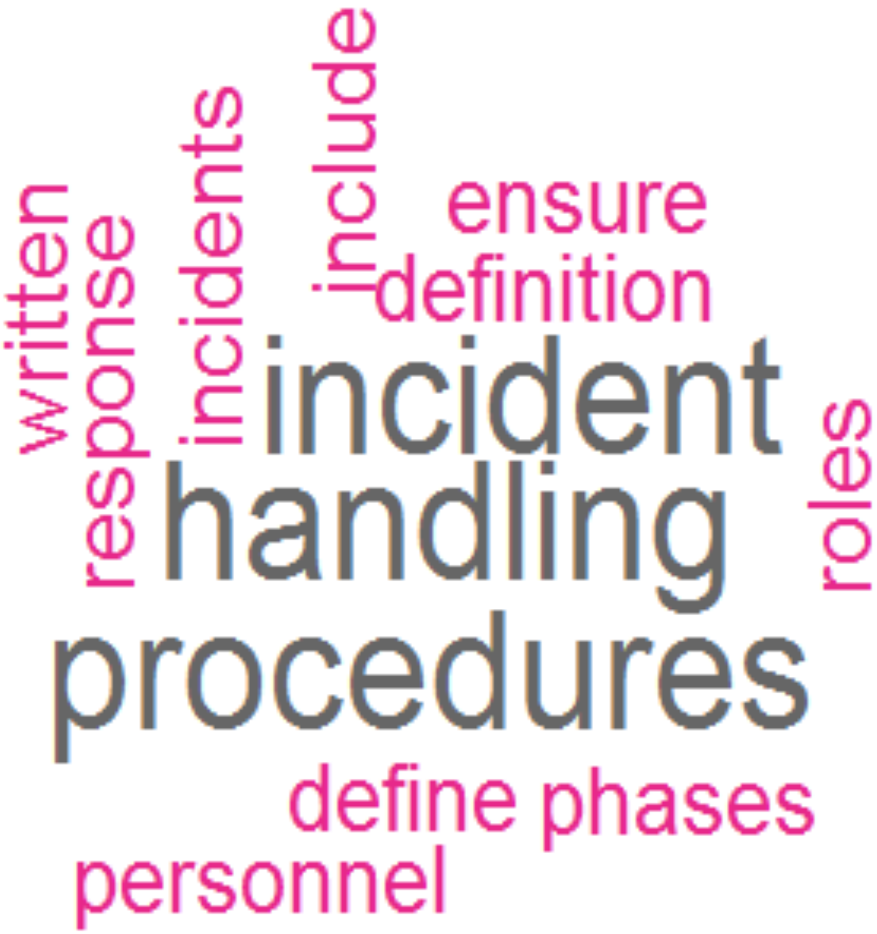
[1] “Critical Security Control #19: Incident Response and Management”

[1]

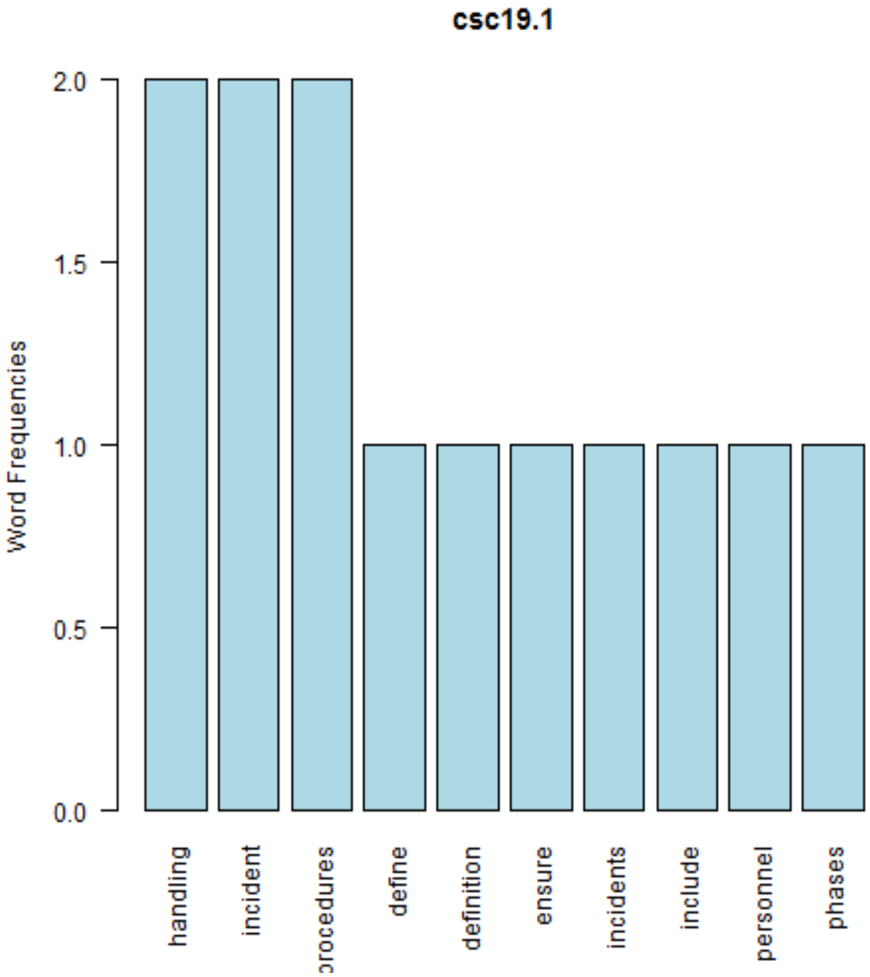
[1] [1] “To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (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 19.1

[1] "handling + incident"



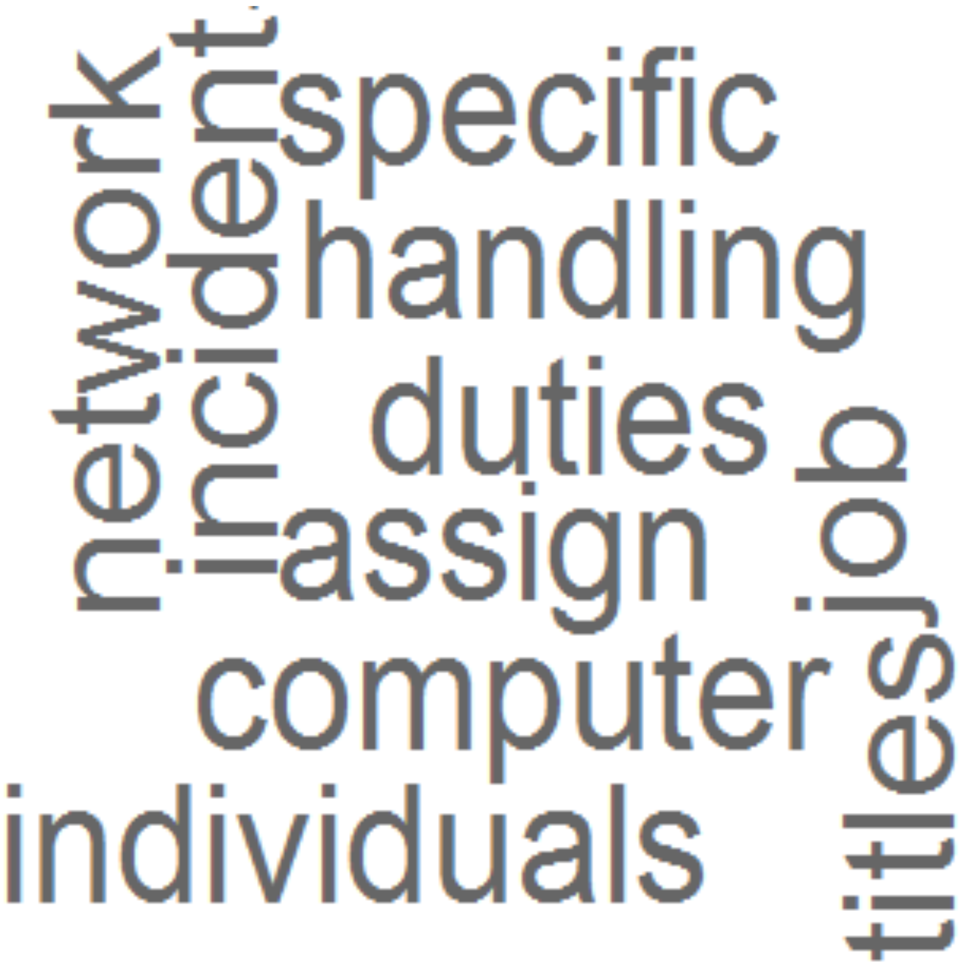
null device 1



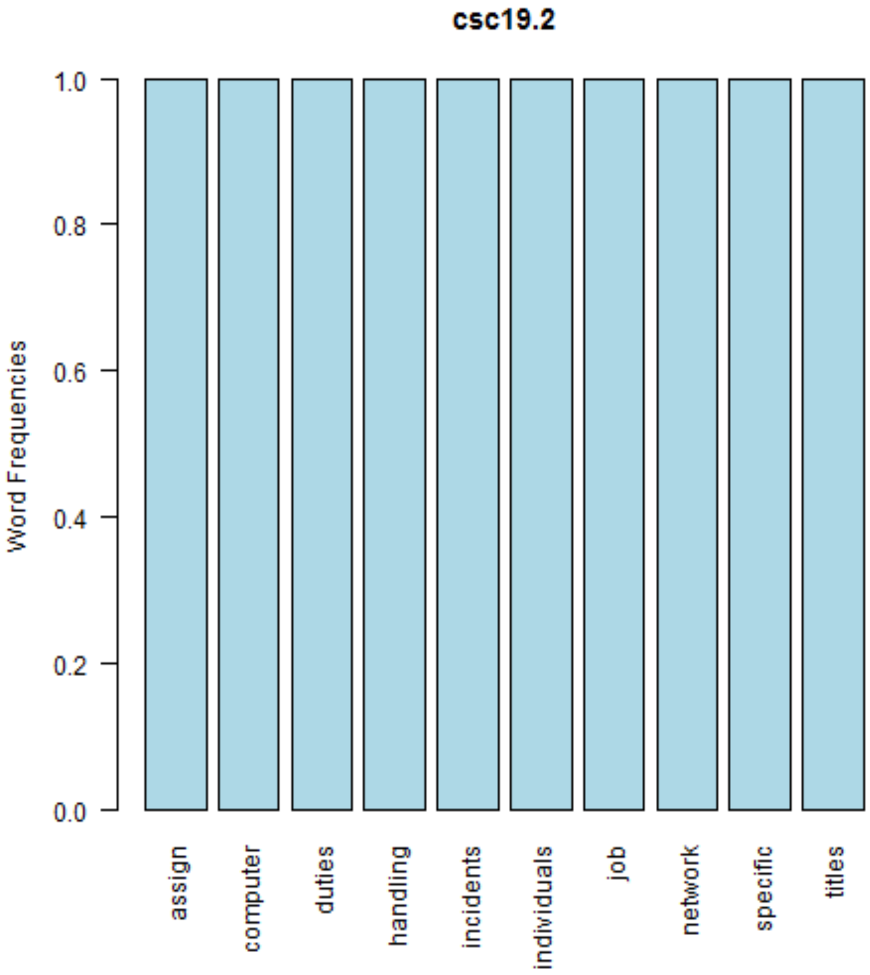
null device 1 [1] "Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling."

CSC 19.2

[1] “assign + computer”



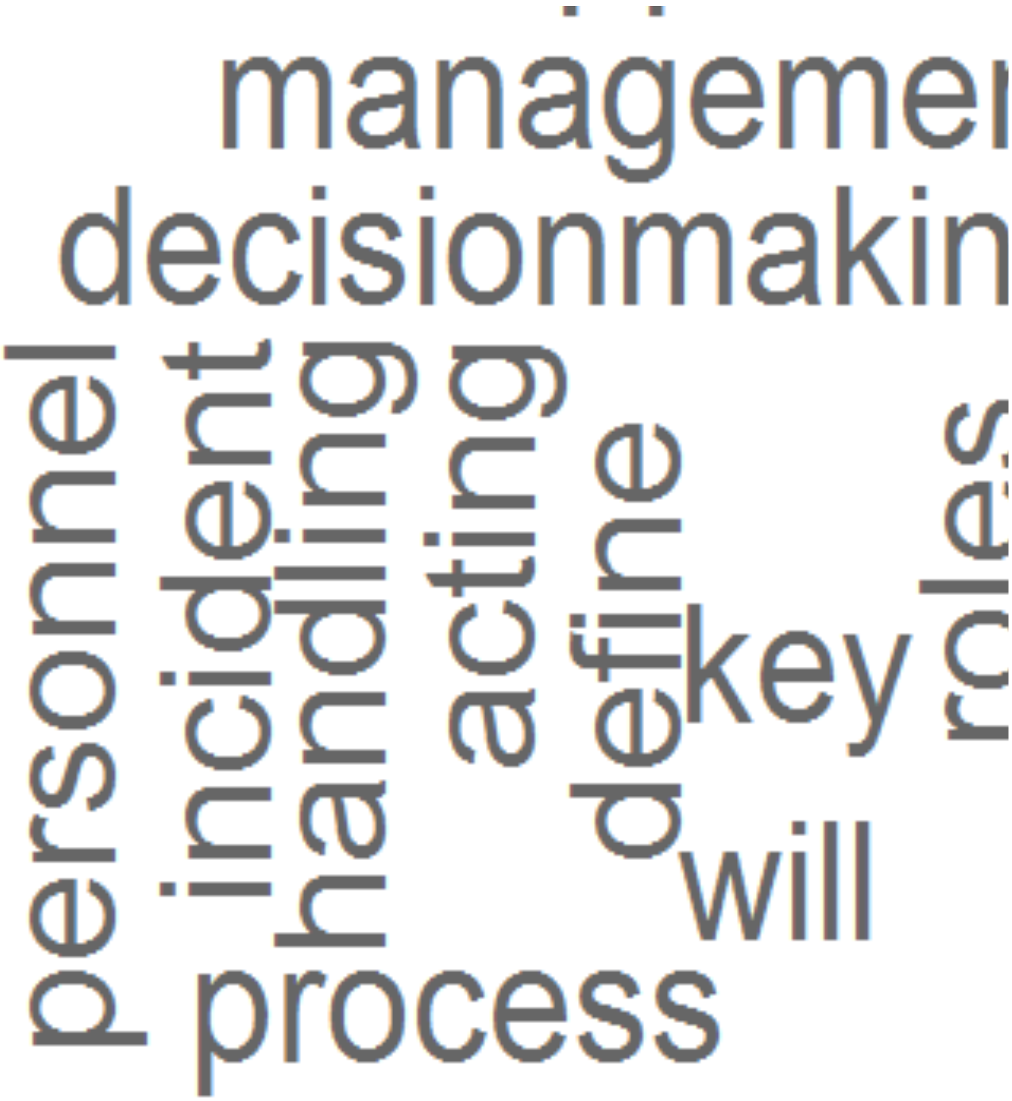
null device 1



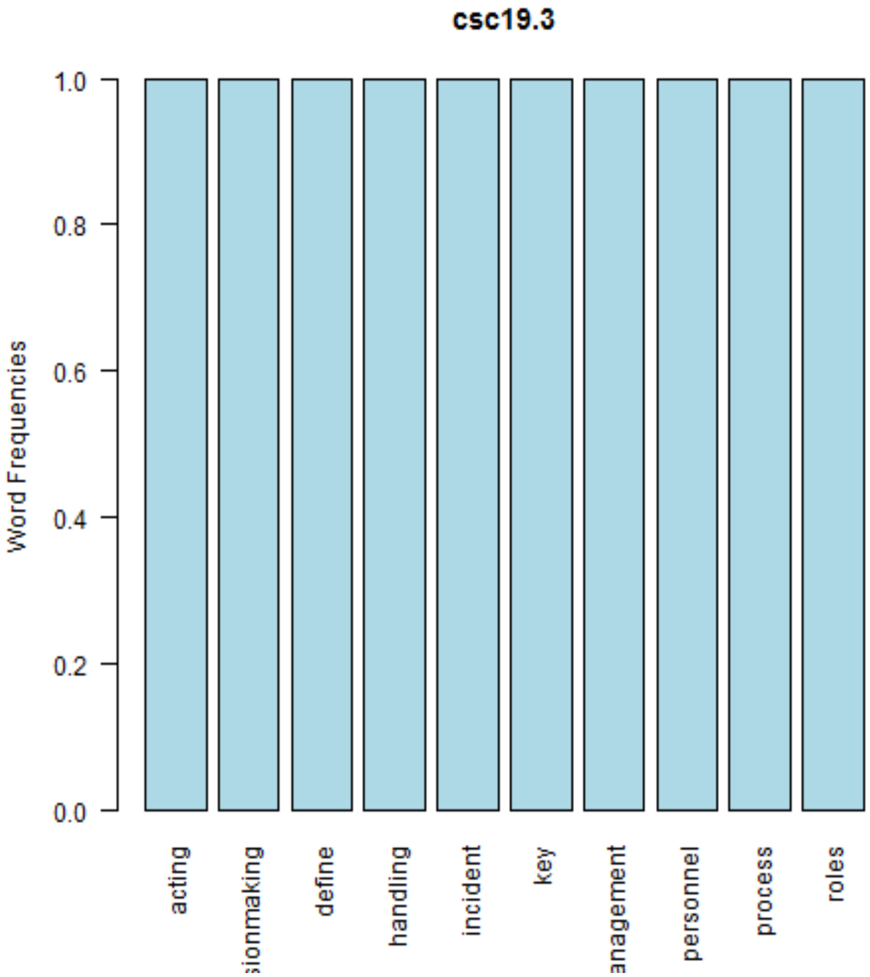
null device 1 [1] "Assign job titles and duties for handling computer and network incidents to specific individuals."

CSC 19.3

[1] “acting + decisionmaking”



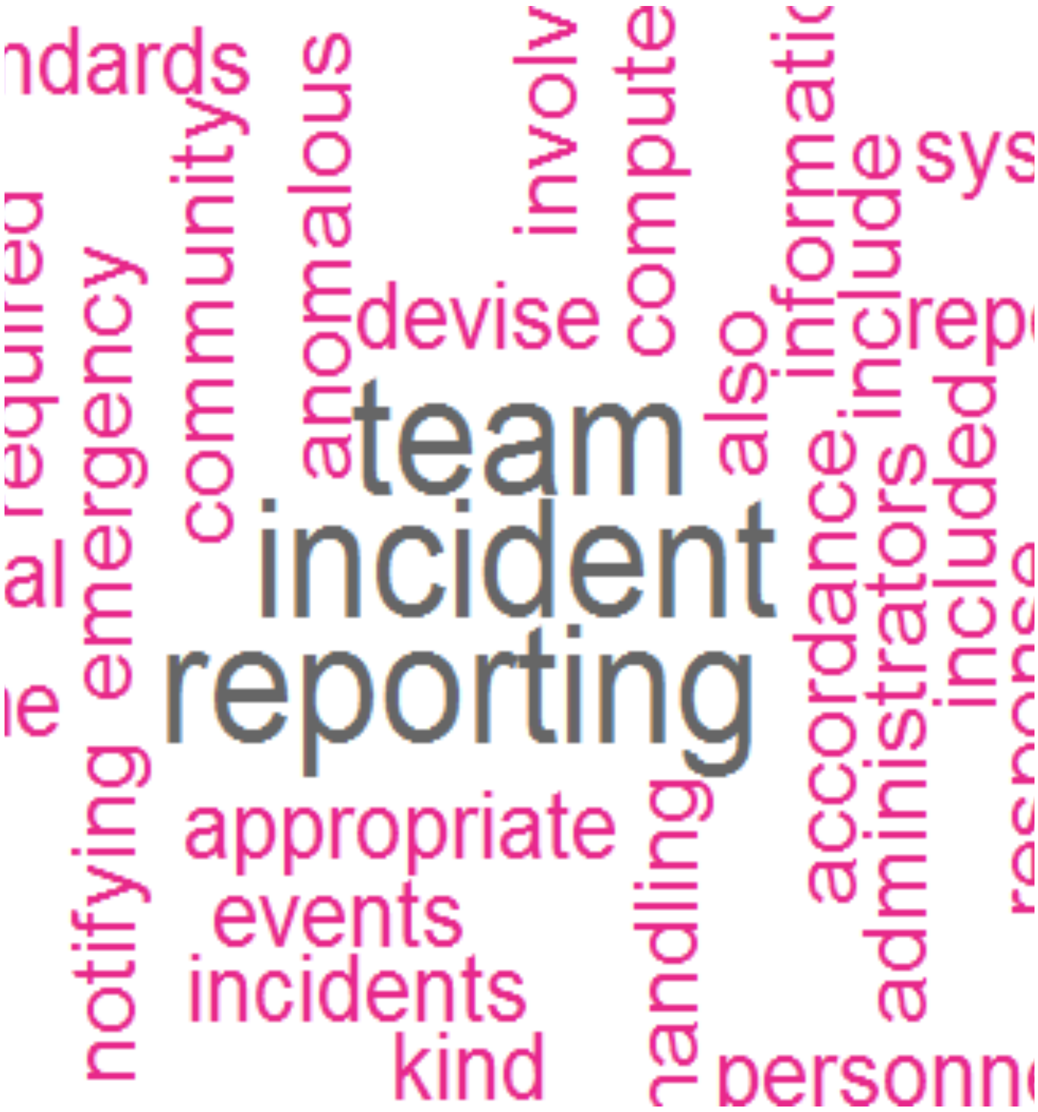
null device 1



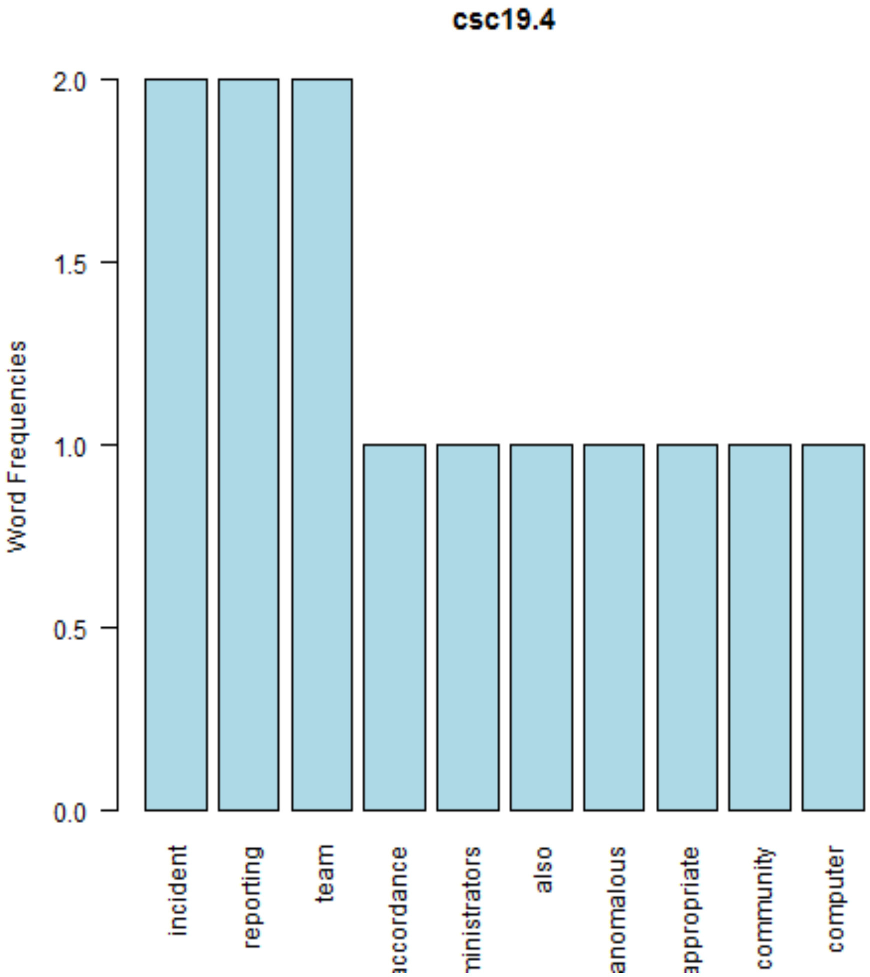
null device 1 [1] "Define management personnel who will support the incident handling process by acting in key decision-making roles."

CSC 19.4

[1] “incident + reporting”



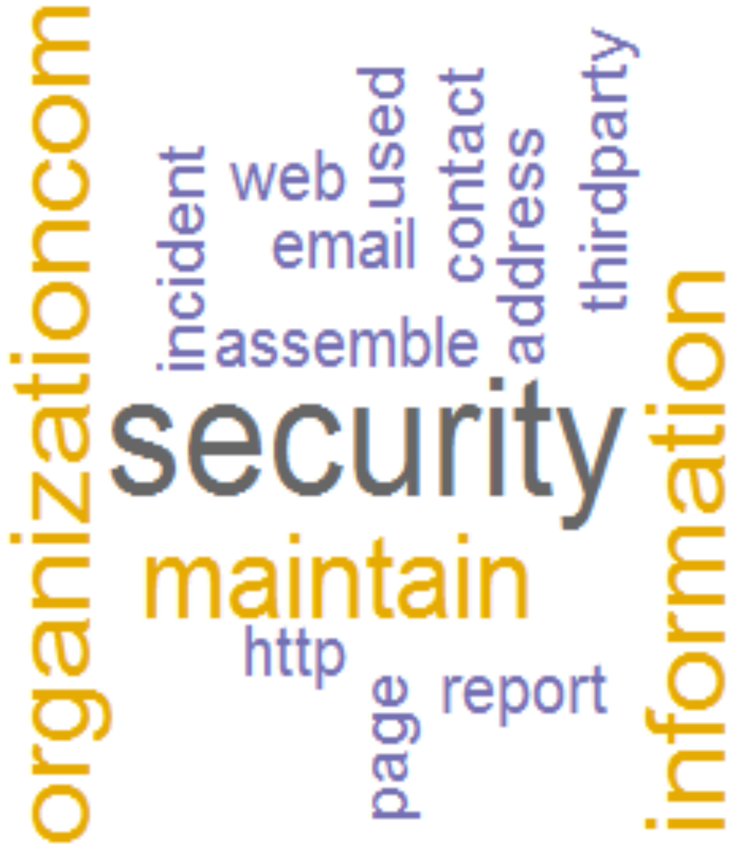
null device 1



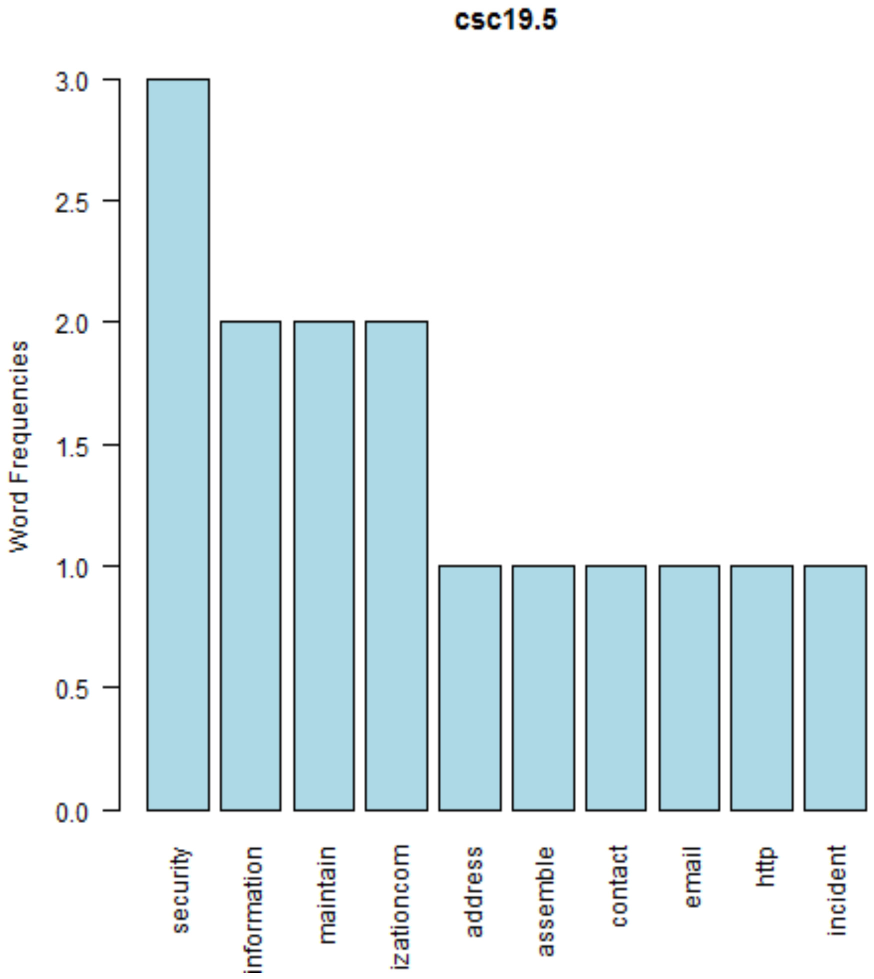
null device 1 [1] “Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.”

CSC 19.5

[1] "security + information"



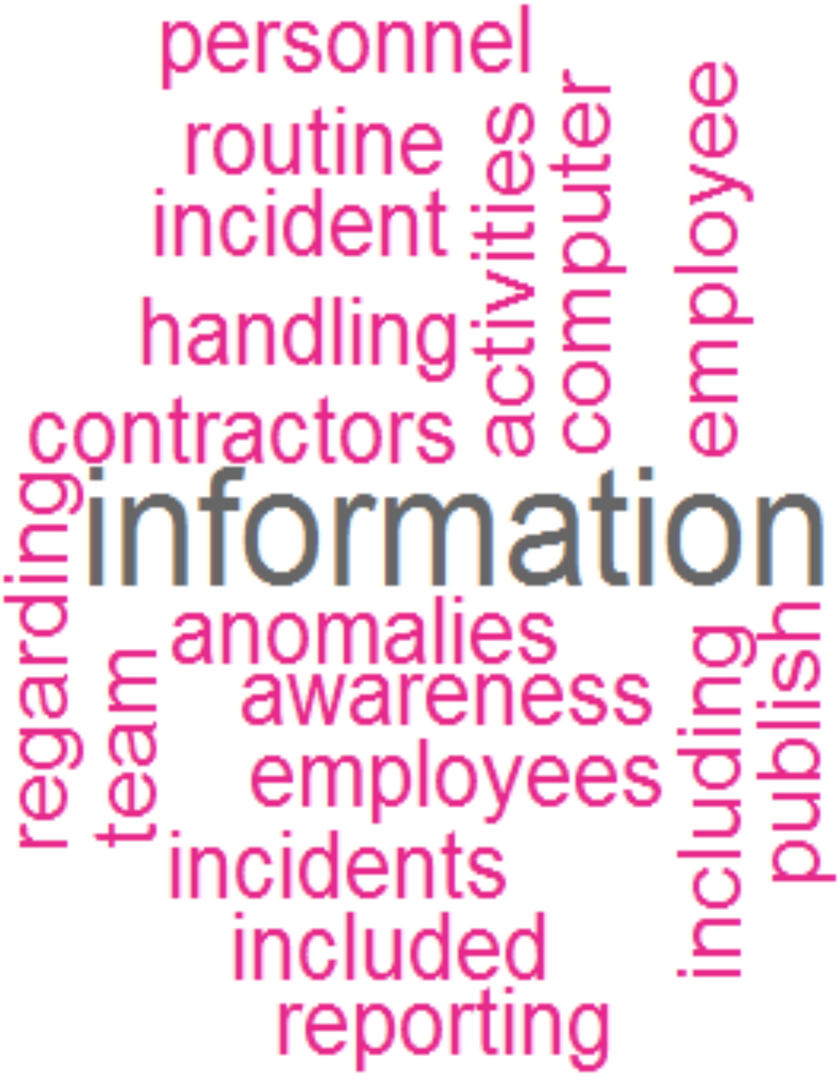
null device 1



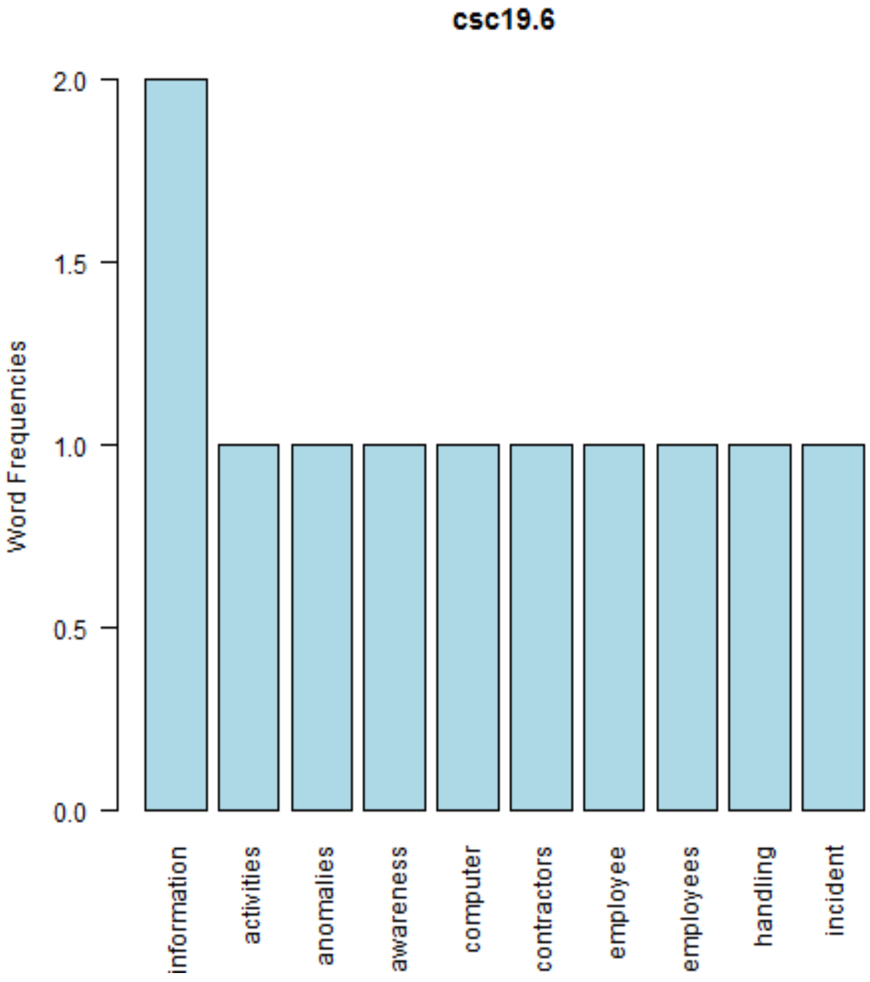
null device 1 [1] “Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).”

CSC 19.6

```
[1] “information + activities”
```



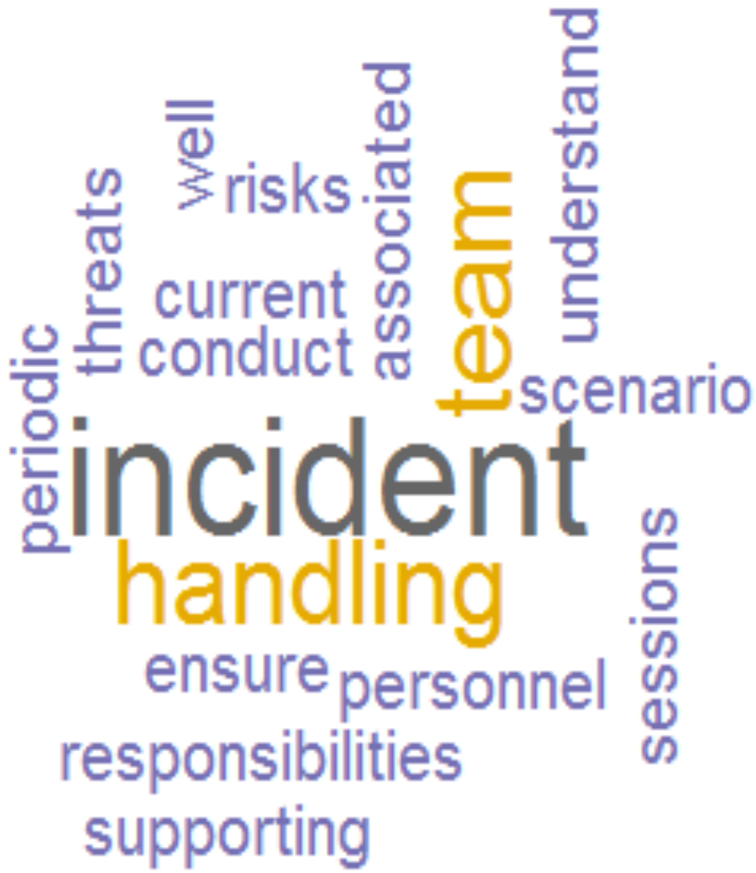
```
null device 1
```



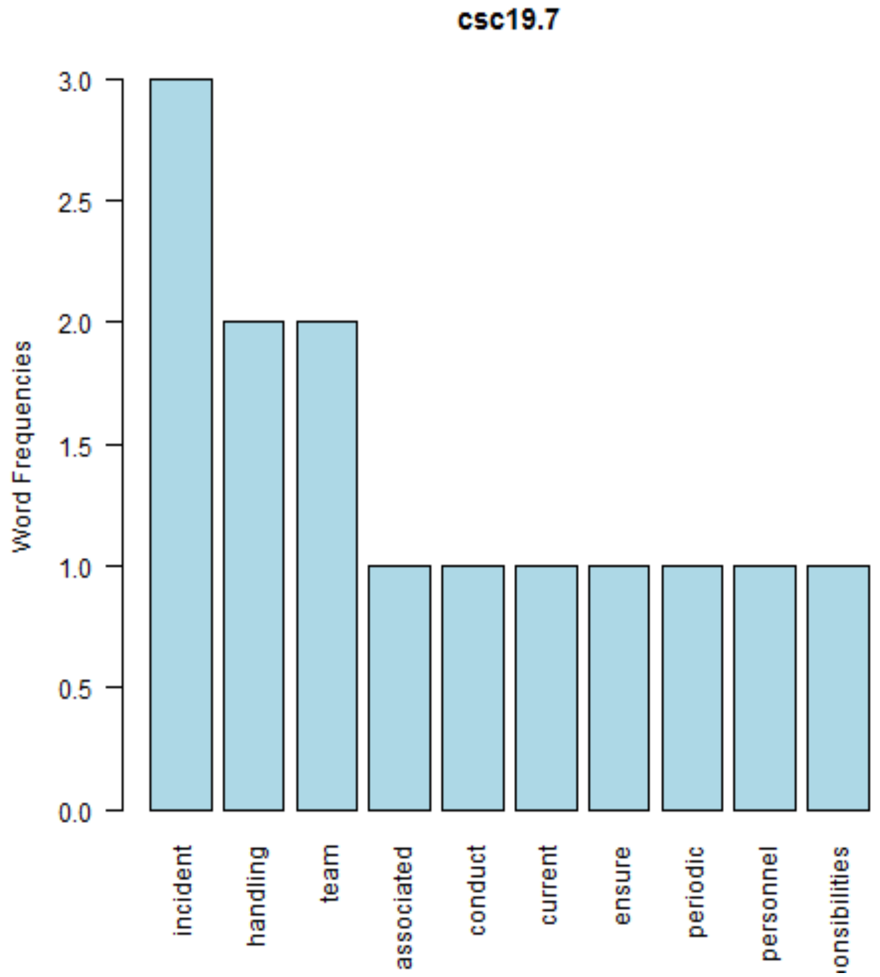
null device 1 [1] “Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.”

CSC 19.7

[1] “incident + handling”



null device 1



null device 1 [1] “Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.”