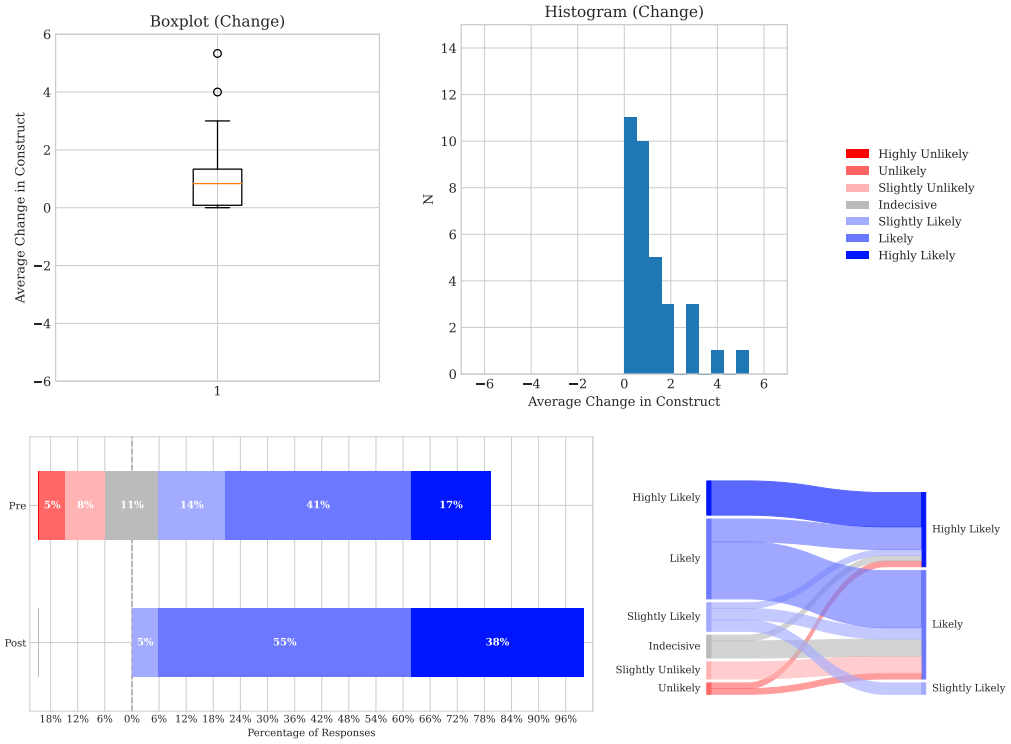
D Graphs

This section contains all visualizations produced as part of the analysis. It is set up such that each page contains all visualizations for a construct and the associated questions.

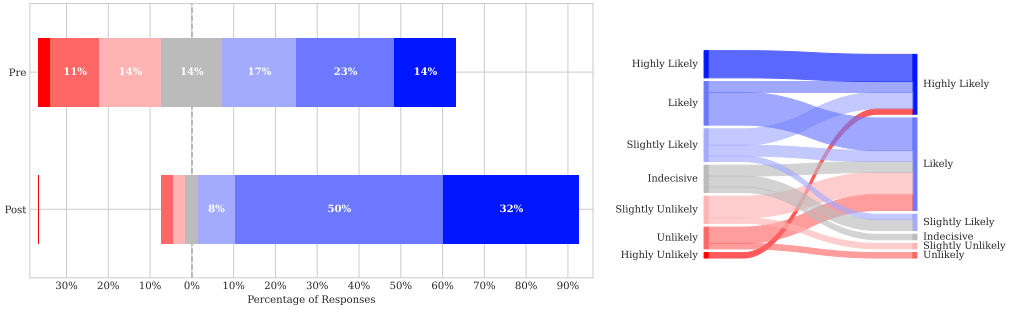
At the top of each page, a box plot and a histogram are, to check for normally distributed data. Next to the histogram, the legend for the visualizations on question level is included.

Beneath the prior mentioned elements, there are a likert-scale distribution and a sankey diagrams for each question belonging to the construct.

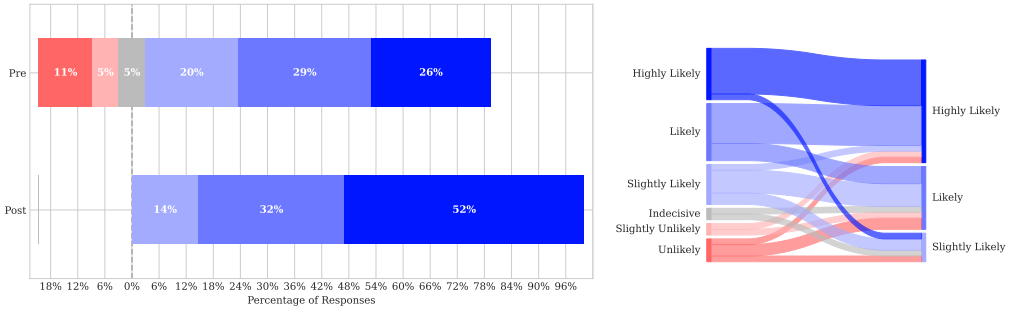
Figure D.1: Perceived probability of security breach



(a) How likely is it that a security violation will cause a significant outage that will result in loss of productivity?

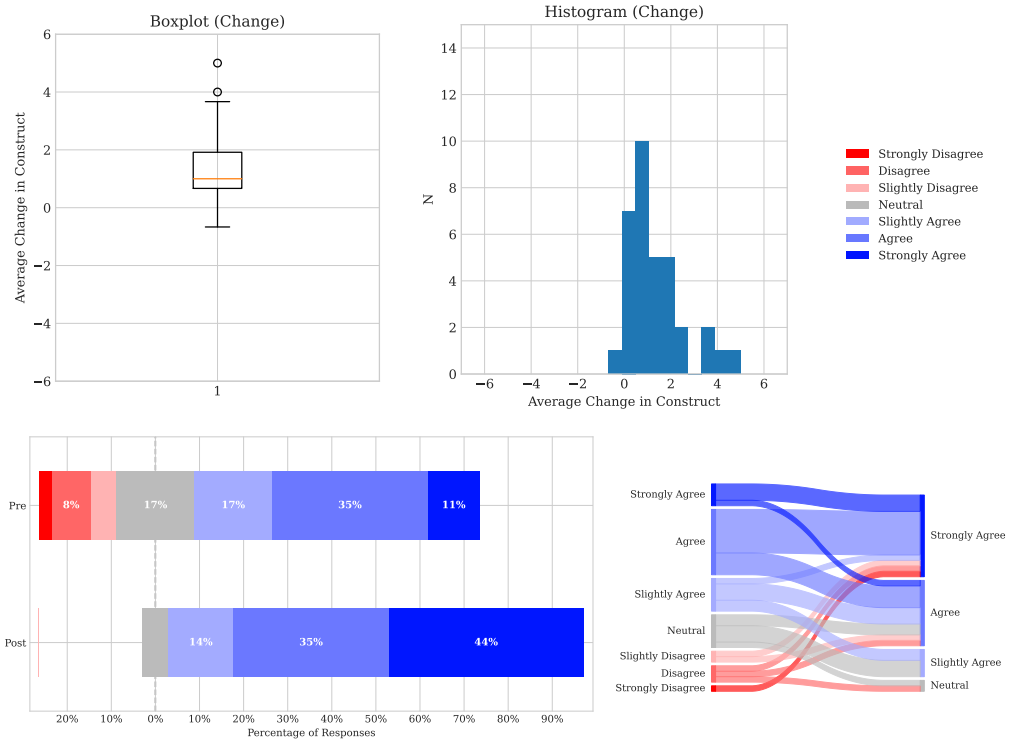


(b) How likely is it that an security violation will cause a significant outage to the internet that results in financial losses to your organization

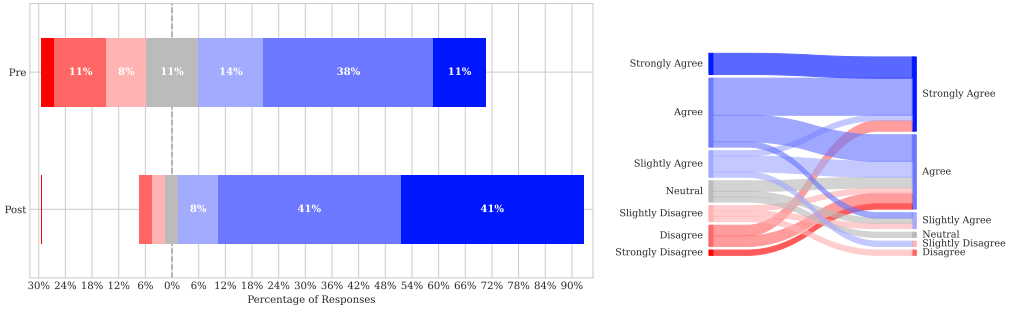


(c) How likely is it that your organization will lose sensitive data due to a security violation?

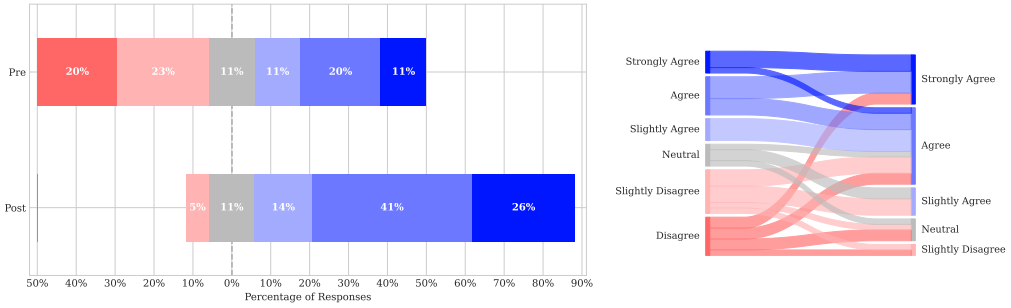
Figure D.2: Perceived severity of security breach



(a) I believe that information stored on my organization's computers is vulnerable to security incidents.

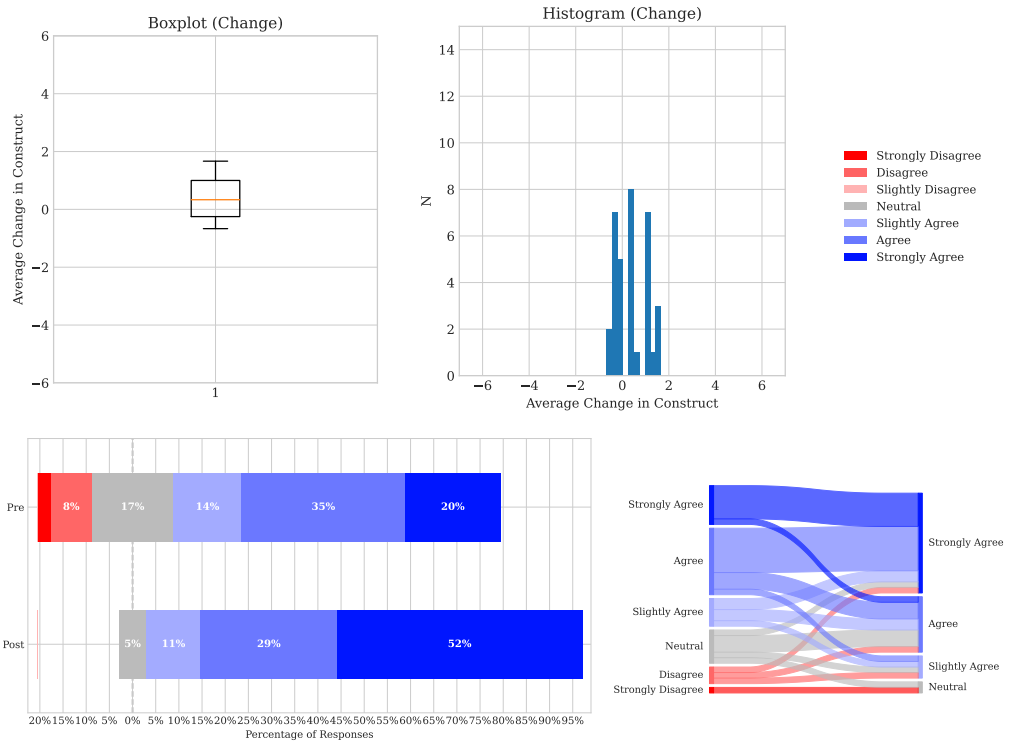


(b) I believe the productivity of my organization and its employees is threatened by security incidents.

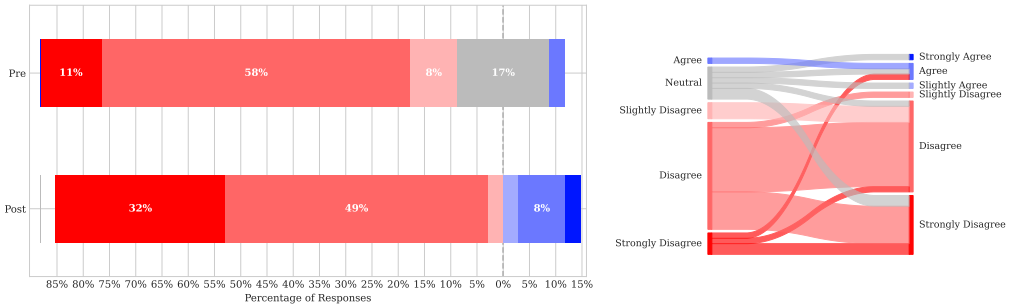


(c) I believe the profitability of my organization is threatened by security incidents.

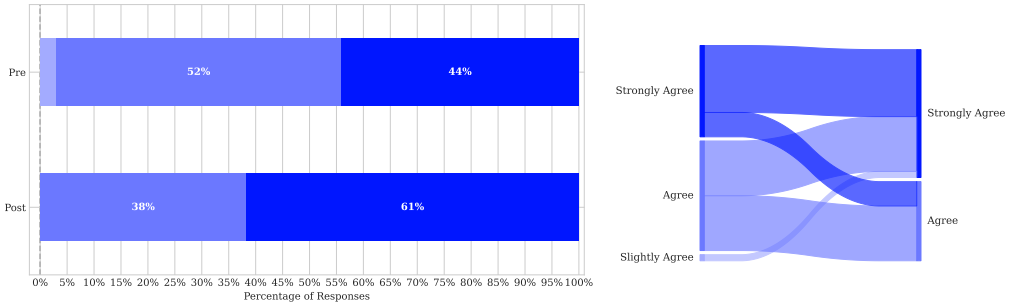
Figure D.3: Security breach concern level



(a) The information systems security issue affects my organization directly.

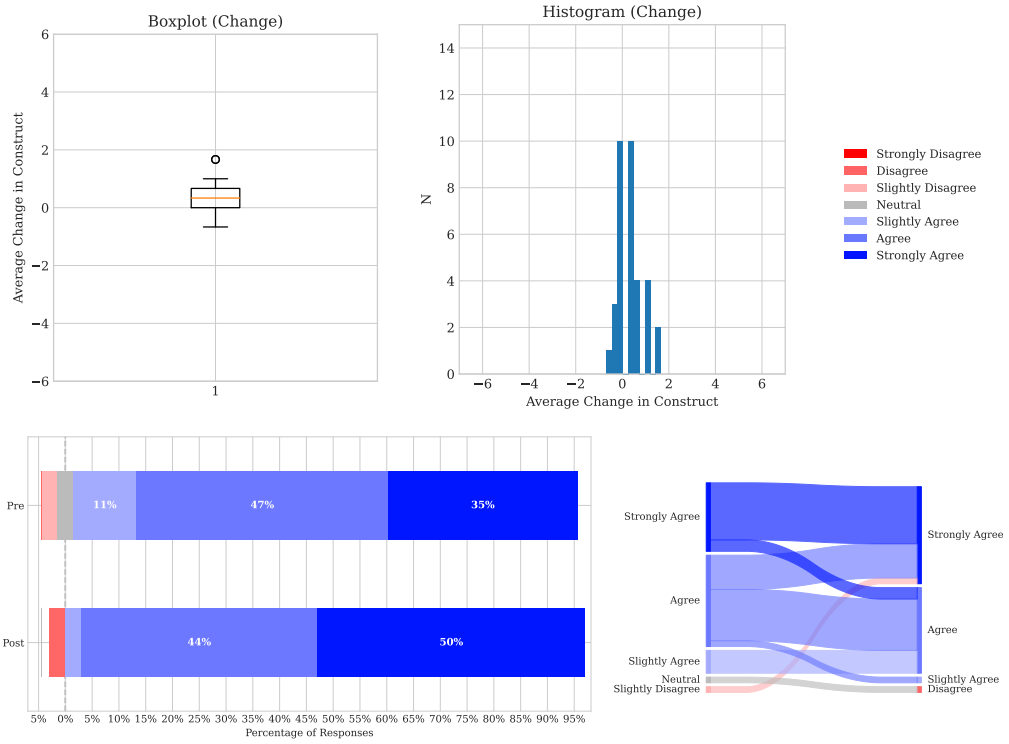


(b) The information systems security issue is exaggerated.

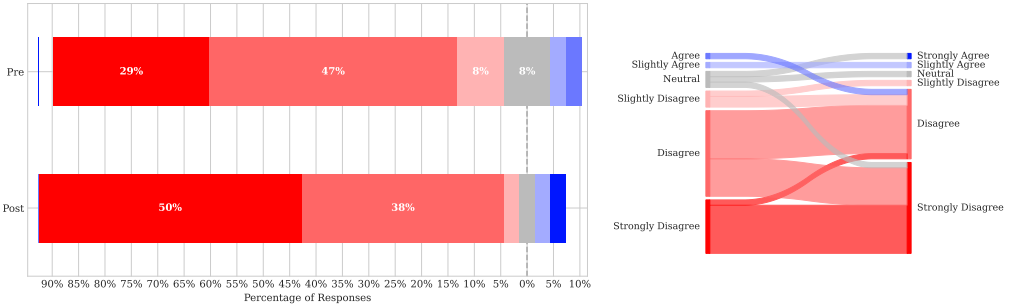


(c) I think information systems security is serious and needs attention.

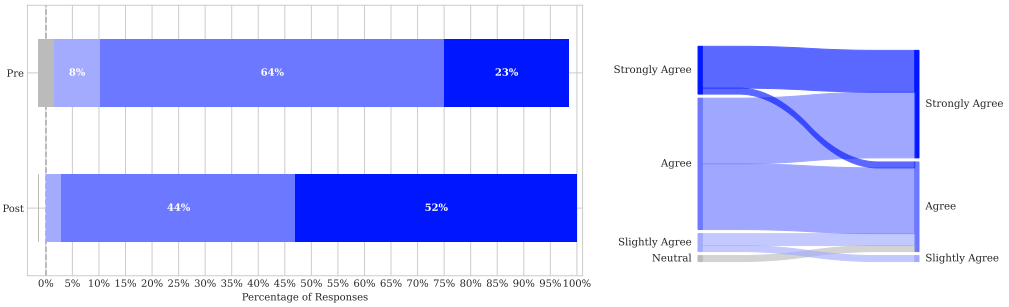
Figure D.4: Response efficacy



(a) Every employee can make a difference when it comes to helping to secure the organisation's information systems.

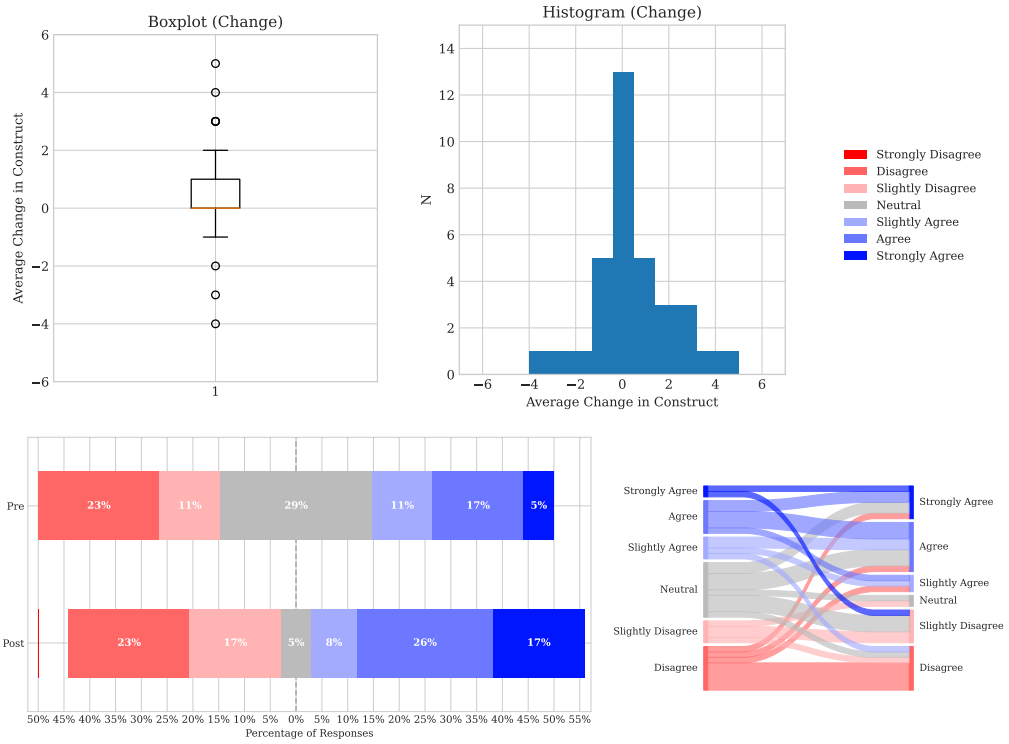


(b) There is not much that any one individual can do to help secure the information systems of my organization.



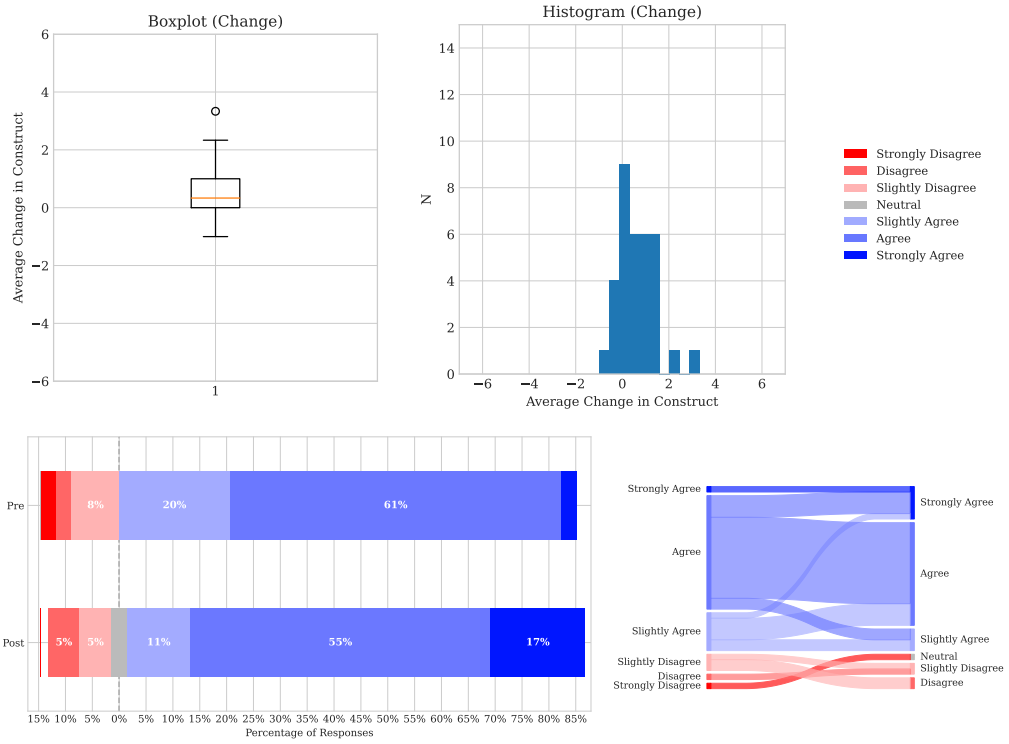
(c) If I follow the organization information systems security policies, I can make a difference in helping to secure my organization's information systems.

Figure D.5: Cost

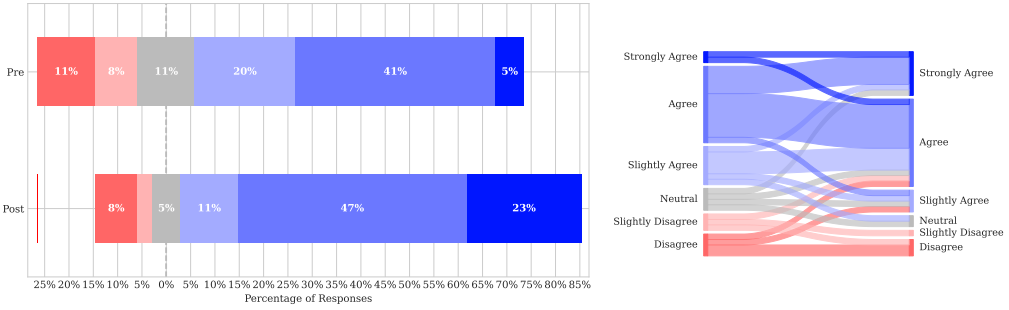


(a) Adopting security technologies and practices poses hindrance.

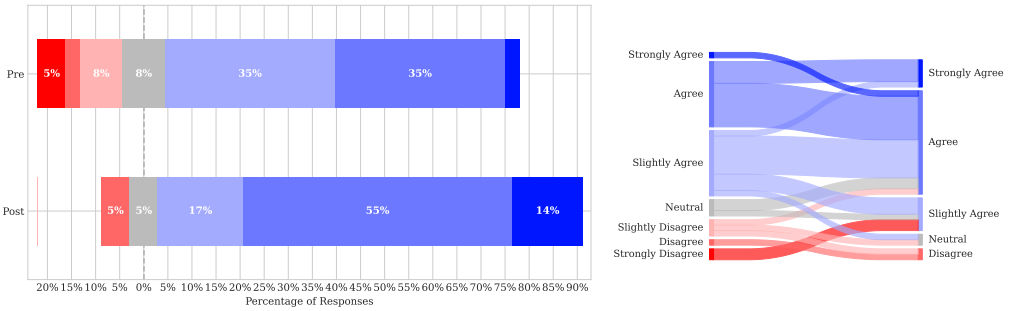
Figure D.6: Self-efficacy



(a) I would feel comfortable following most of the information systems security policies on my own.

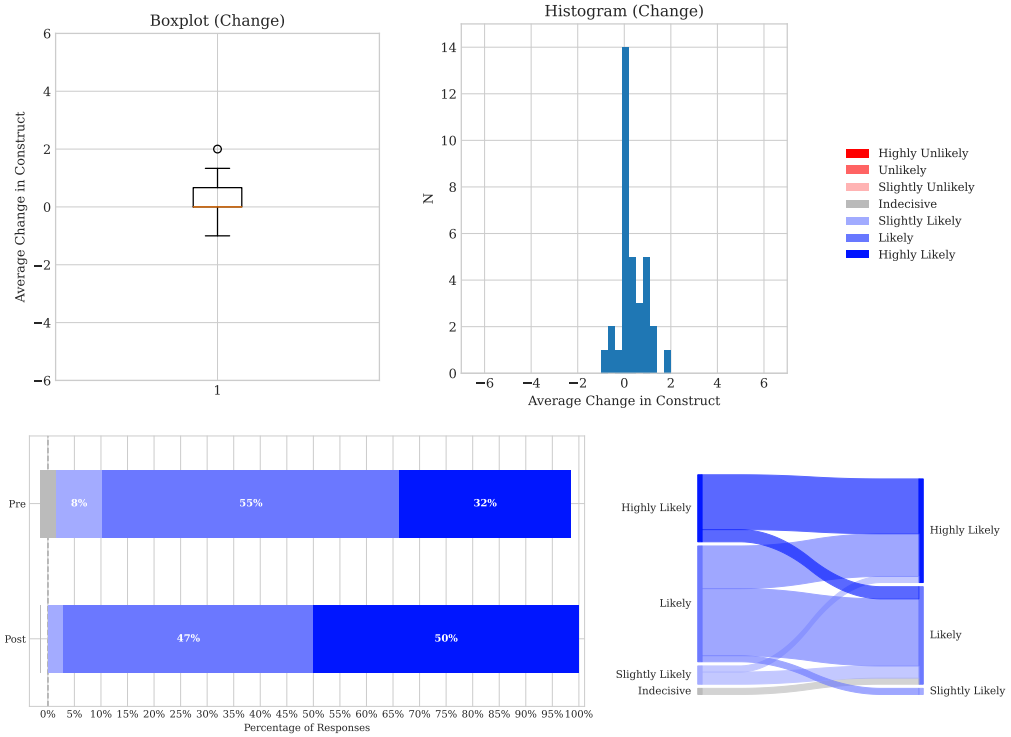


(b) If I wanted to, I could easily follow information systems security policies on my own.

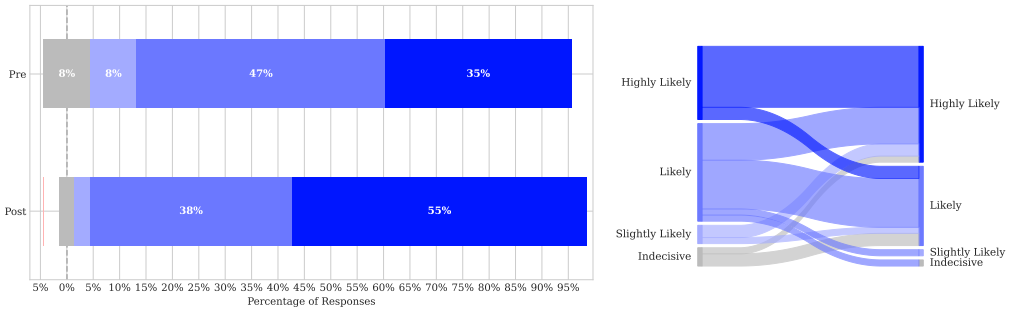


(c) I would be able to follow most of the information systems security policies even if there was no one around to help me.

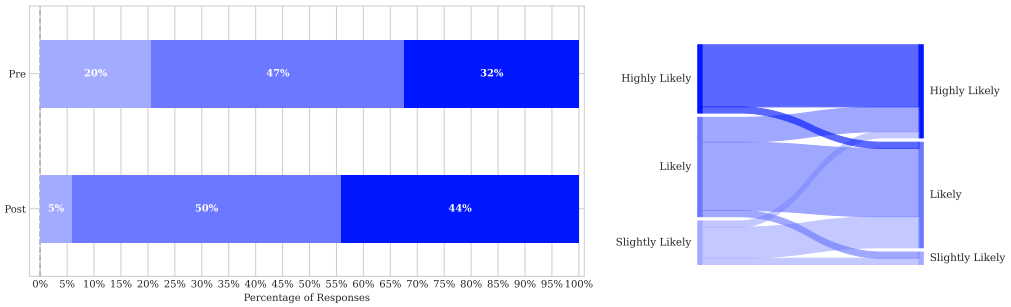
Figure D.7: Security policy compliance intention



(a) I am likely to follow organisational security policies.

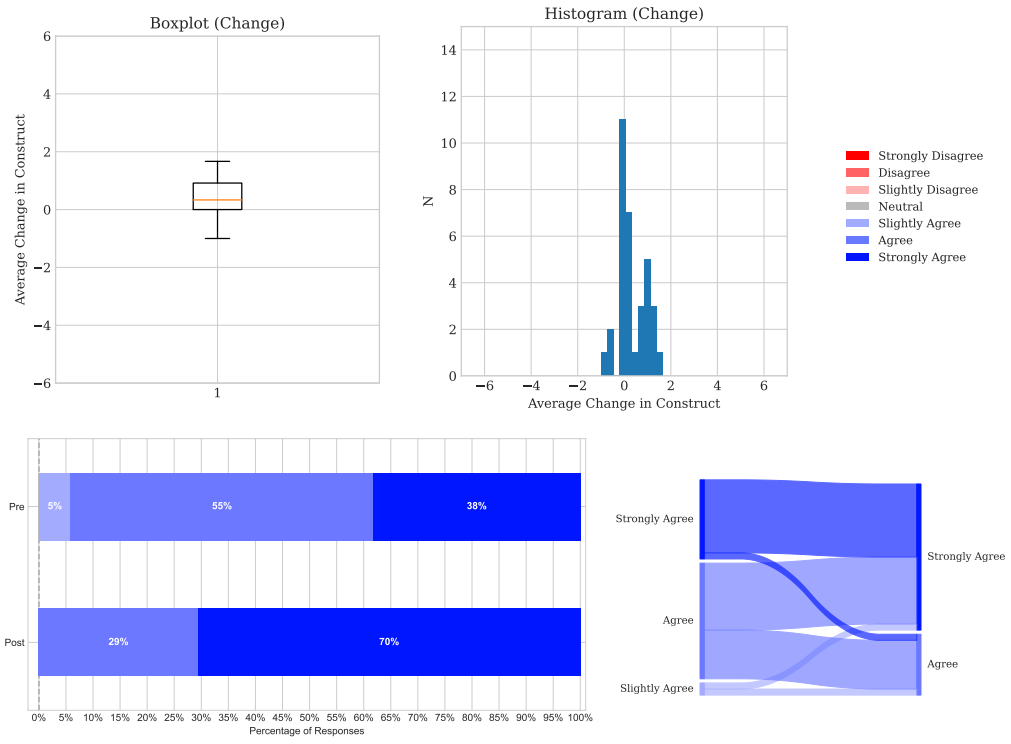


(b) It is possible that I will comply with organisational information systems security policies to protect the organisation's information systems.

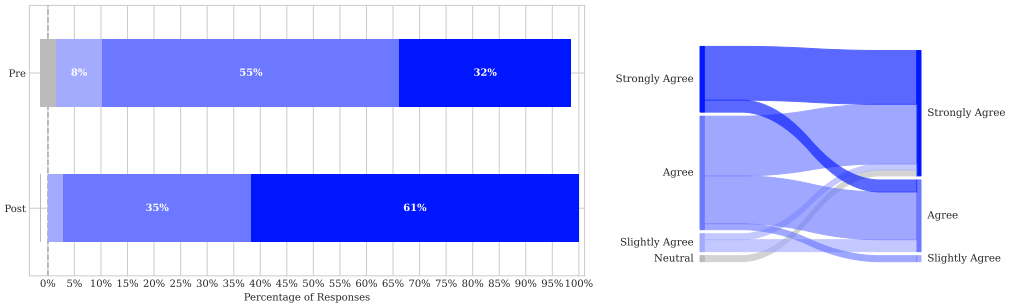


(c) I am certain that I will follow organisational security policies.

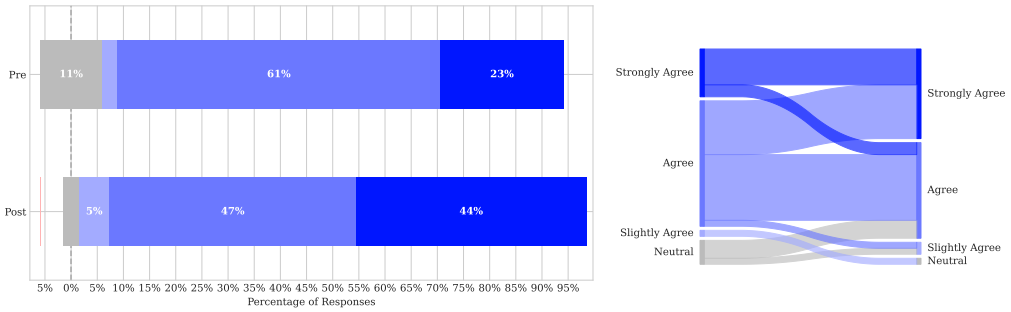
Figure D.8: Security policy attitude



(a) I am certain that I will follow organisational security policies.



(b) Adopting security technologies and practices is important.



(c) Adopting security technologies and practices is beneficial.