Barometer Survey: IT Security

A Register Reader Study

May 2005

(3,097 Respondents)

Background

- This slide set presents the results of an online survey executed in March 2005 via The Register news site.
- The title of the survey was “IT Security Barometer Survey.” It was publicised via The Register site itself and via an email invitation sent to a panel of pre-registered respondents.
- The questionnaire used was designed by Quocirca Ltd, who also analysed and annotated the results appearing in the remainder of this document.
- Note that this study was based on what’s known in research circles as a “self selecting sample”. This essentially means that respondents chose whether or not to participate based on their level of interest in the topic.
- A more complete report with full discussion entitled “Security Barometer Survey” is available from: www.quocirca.com/report_barom_sec.htm (free of charge)

Conclusions

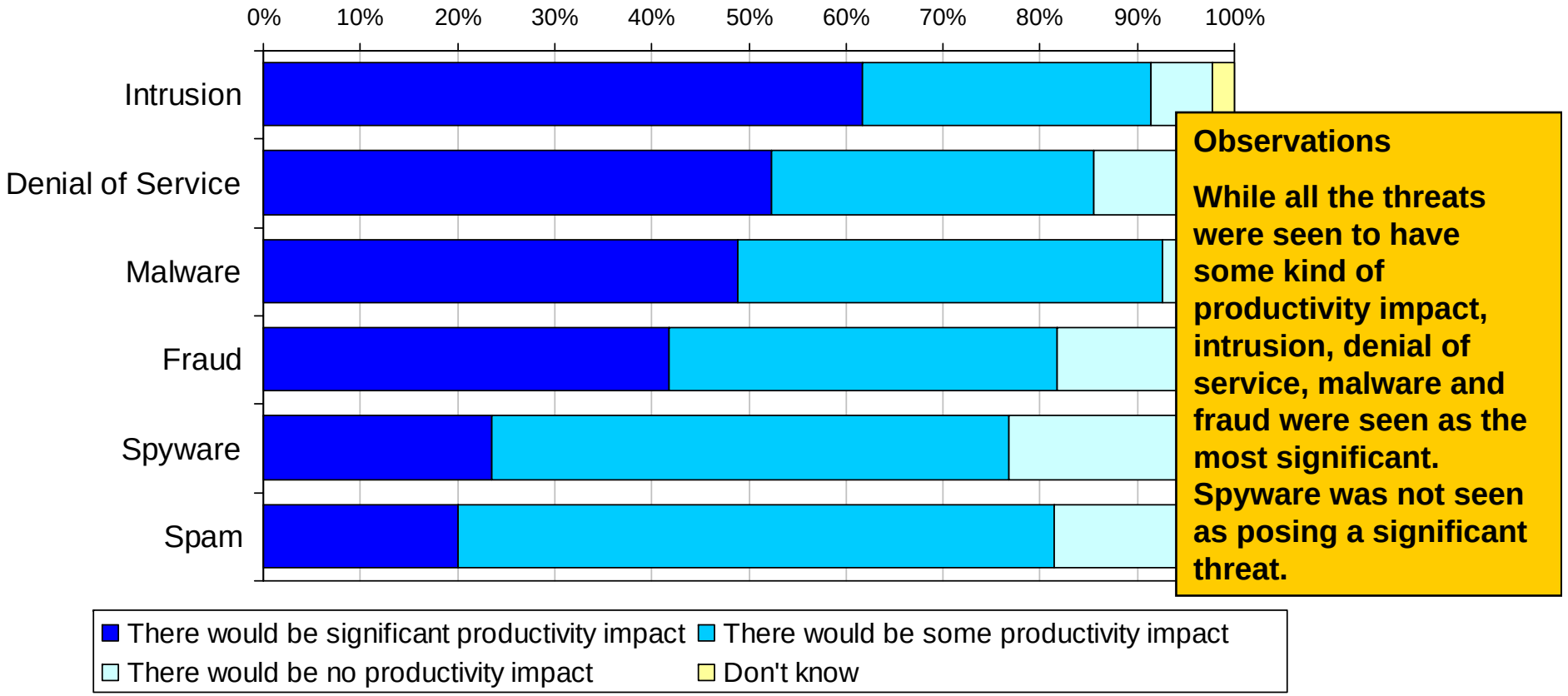
- **Security understanding is still victim to the fear factor**
  In this post downturn age of IT, we would hope that security understanding replicates the increased drive we see towards IT efficiency and effectiveness. However there is considerable evidence that psychological factors are as important as they ever were. For example, companies that suffered a security attack in the recent past, are significantly more aware they might suffer a similar attack in the future. Meanwhile, newer threats such as Spyware are – incorrectly – not yet seen as high risk.

- **Policy-based security enhances awareness**
  It should be expected that companies that take a policy-based, proactive stance on security issues, such as companies who have implemented a formal security policy, would be better protected against security threats. The research seems to show that having a full policy and having no policy makes little difference – however, the analysis shows that this is down to lack of awareness of possible threats from those with no policy in place.

- **Security threats are being hyped above those of unscheduled downtime**
  Roughly three times as many respondents had experienced unscheduled downtime due to software or hardware failure, compared to downtime due to security issues. We should not downplay the issues caused by security, indeed, some system failures may be caused by security problems without it being that obvious. However, companies should be treating downtime in the round.

- **Security issues are directly impacting individual productivity**
  Respondents were quick to point out that there would be significant or some impact of security issues, on either their individual productivity or as a cost to the business. Indeed, over half of respondents considered that they wasted a day or so every month dealing with security issues. This equates to a significant financial cost to industry. A proportion of respondents (at least 10%) have suffered the impact of some kind of security attack in the past three months.

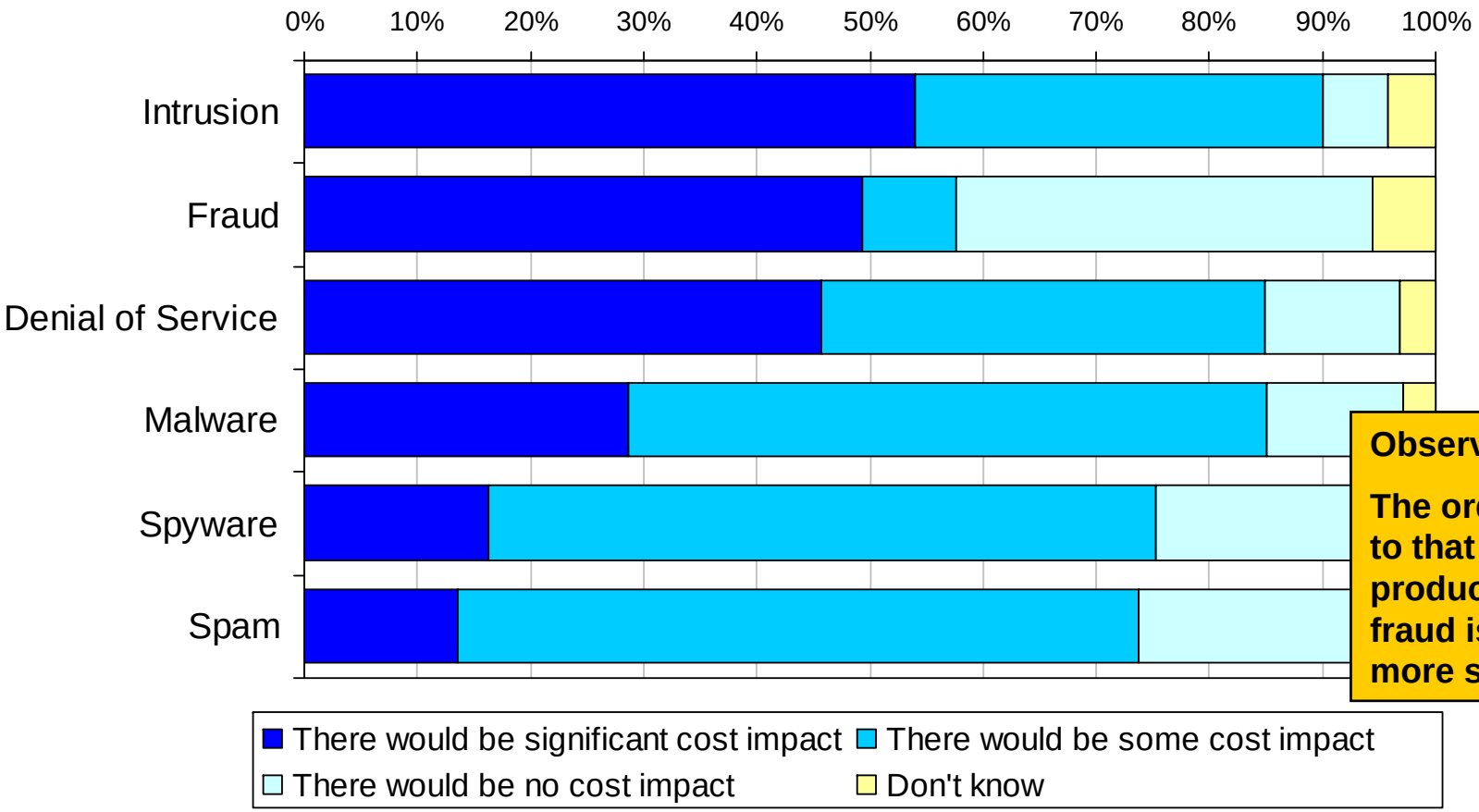
How would you rank the potential impact to your organisation's productivity from the following threats?



Observations

While all the threats were seen to have some kind of productivity impact, intrusion, denial of service, malware and fraud were seen as the most significant. Spyware was not seen as posing a significant threat.

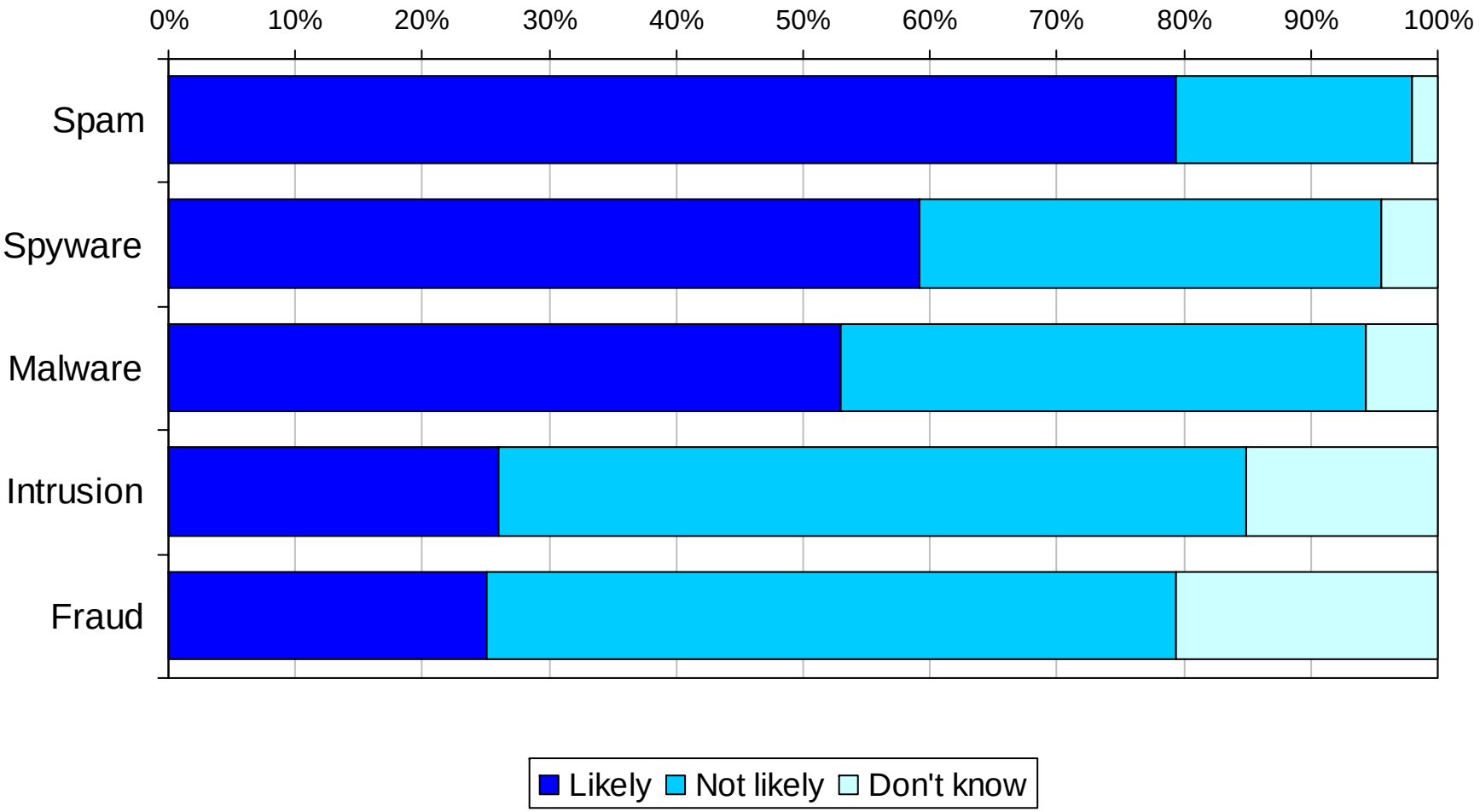
How would you rank the potential cost impact to your organisation?



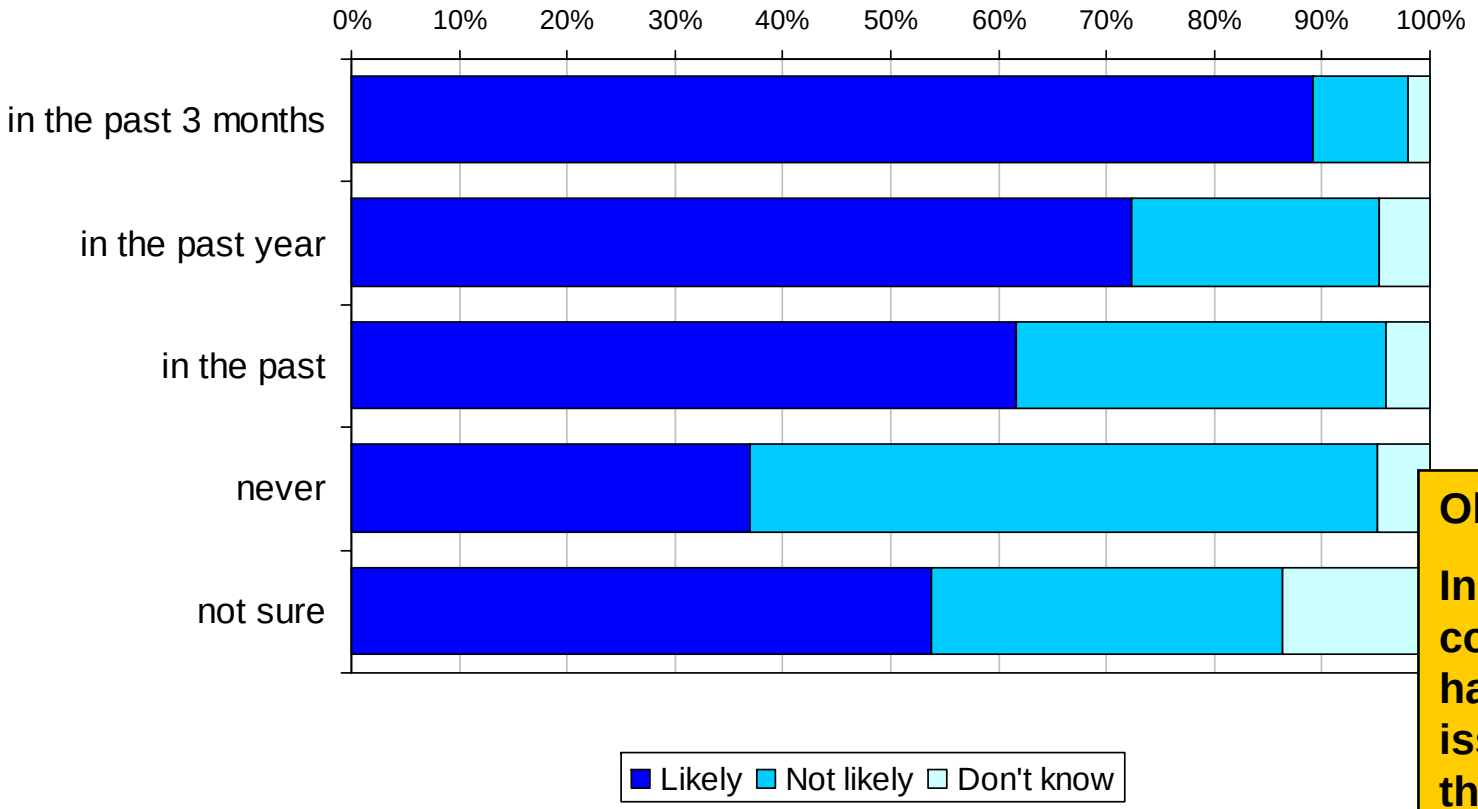
Observations

The order is similar to that with productivity, but fraud is seen as more significant.

How would you rank the likelihood of the following occurring in the future?



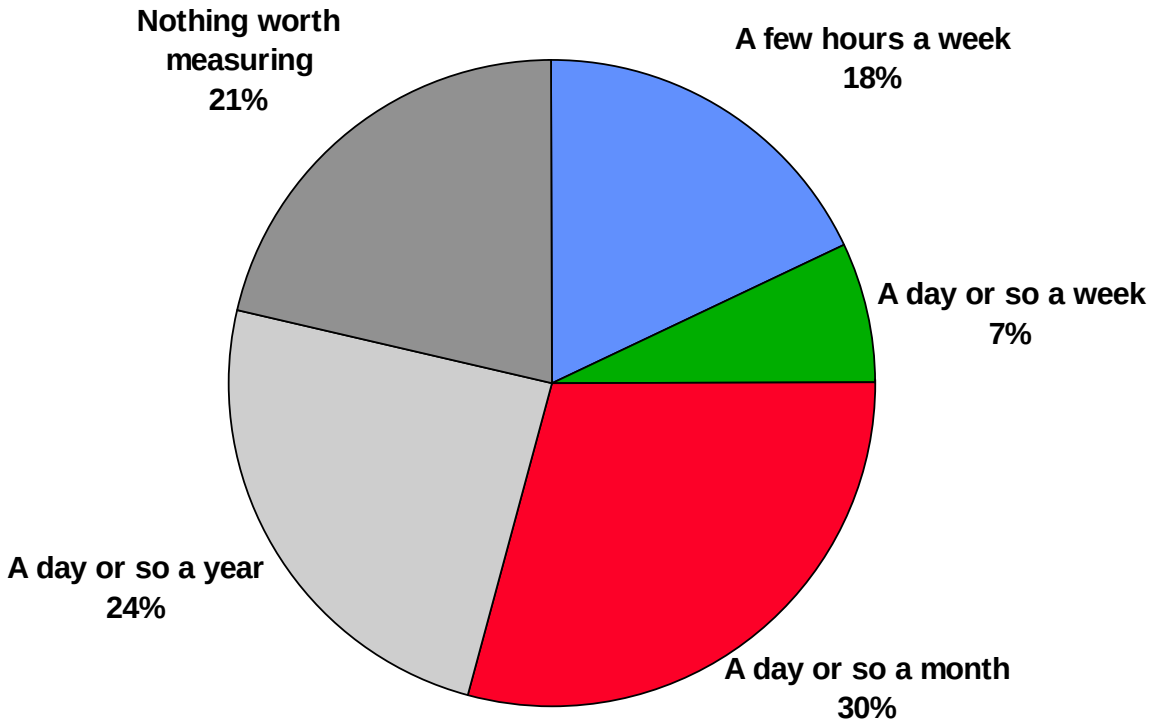
If you have experienced such a threat in the past, how would you rank the likelihood of Malware in the future?



Observations

In every case, companies who have experienced an issue seem to take the threat more seriously.

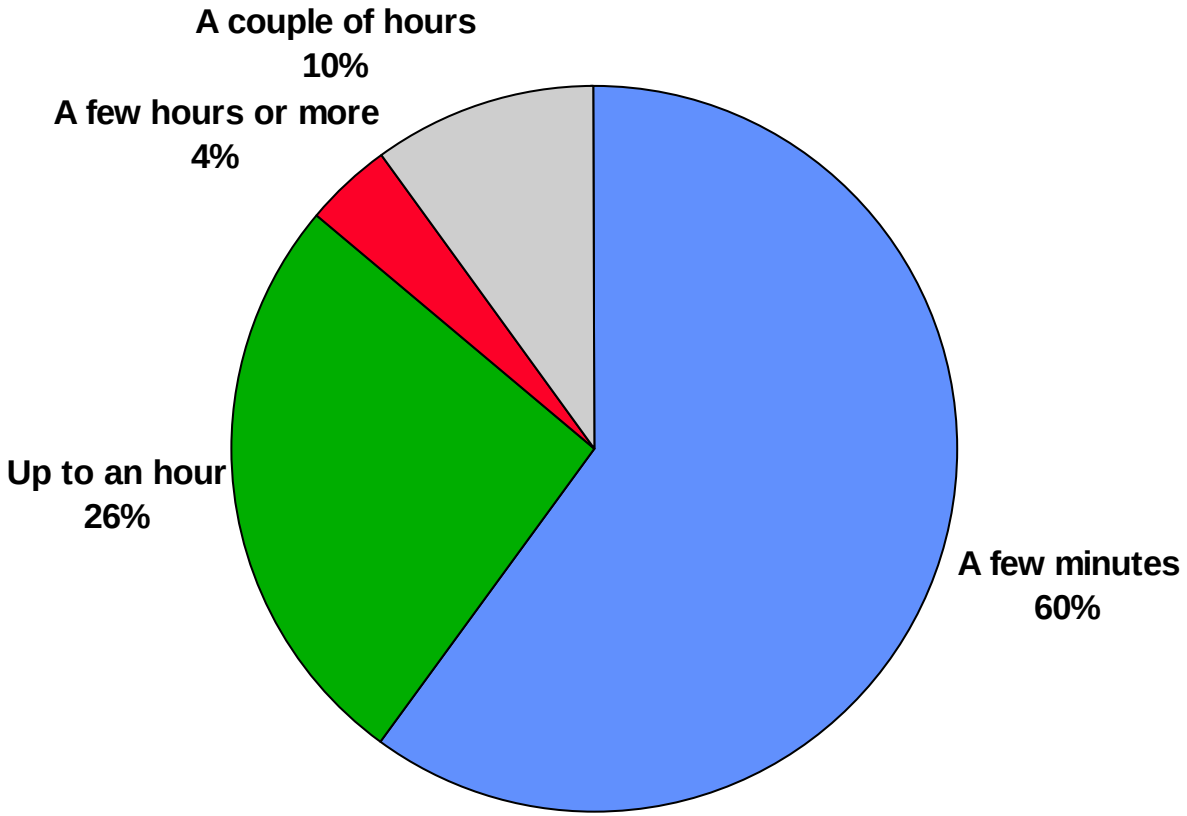
How much time would you consider you waste due to security problems?



Observations

Over half of respondents – 55% – felt they wasted at least a day per month (about 1 day in 20) due to security problems. This is a significant finding.

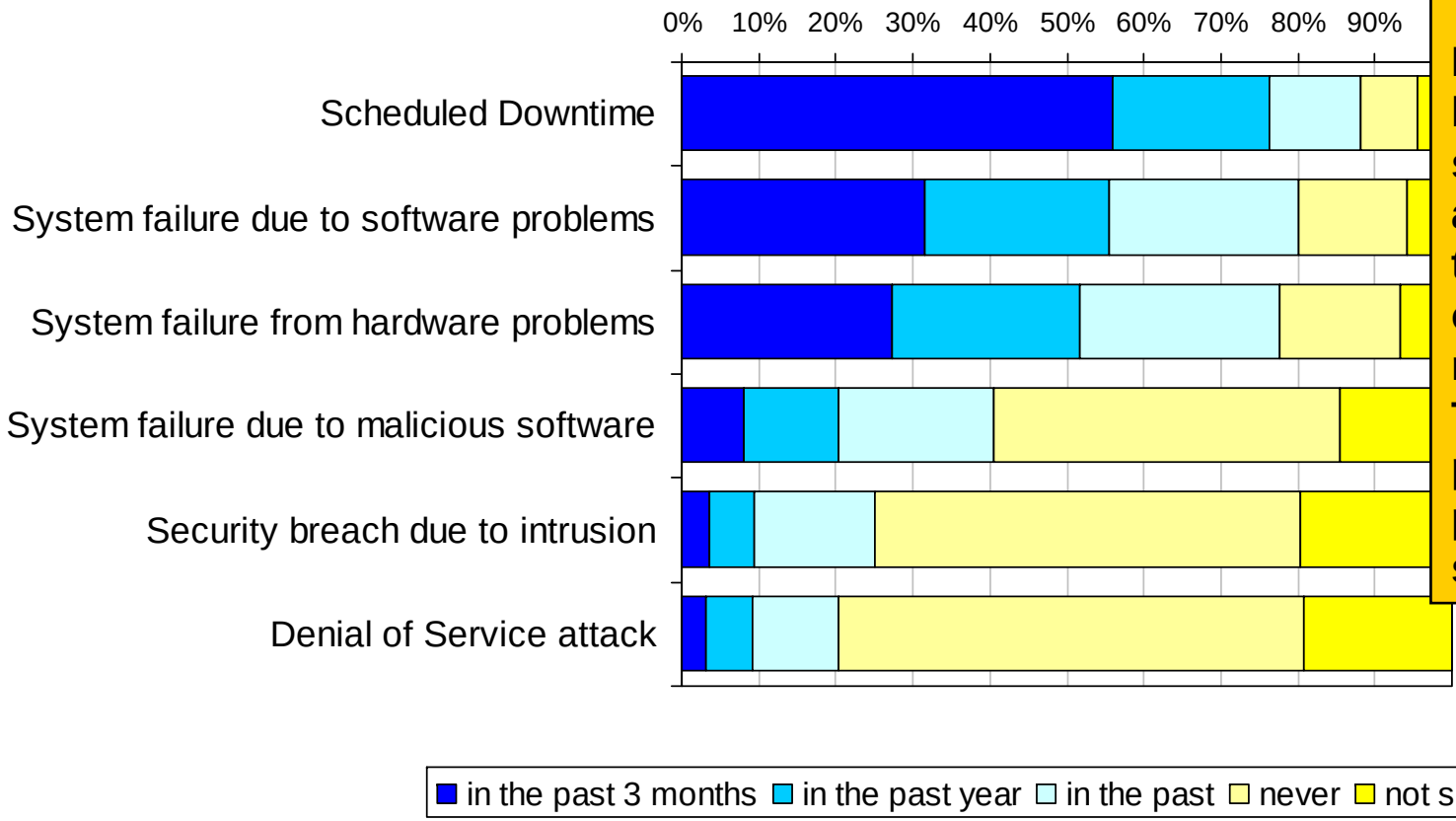
How much time do you personally spend per week dealing with Spam?



Observations

While only 14% of respondents wasted more than an hour on Spam per week, clearly it remains an issue .

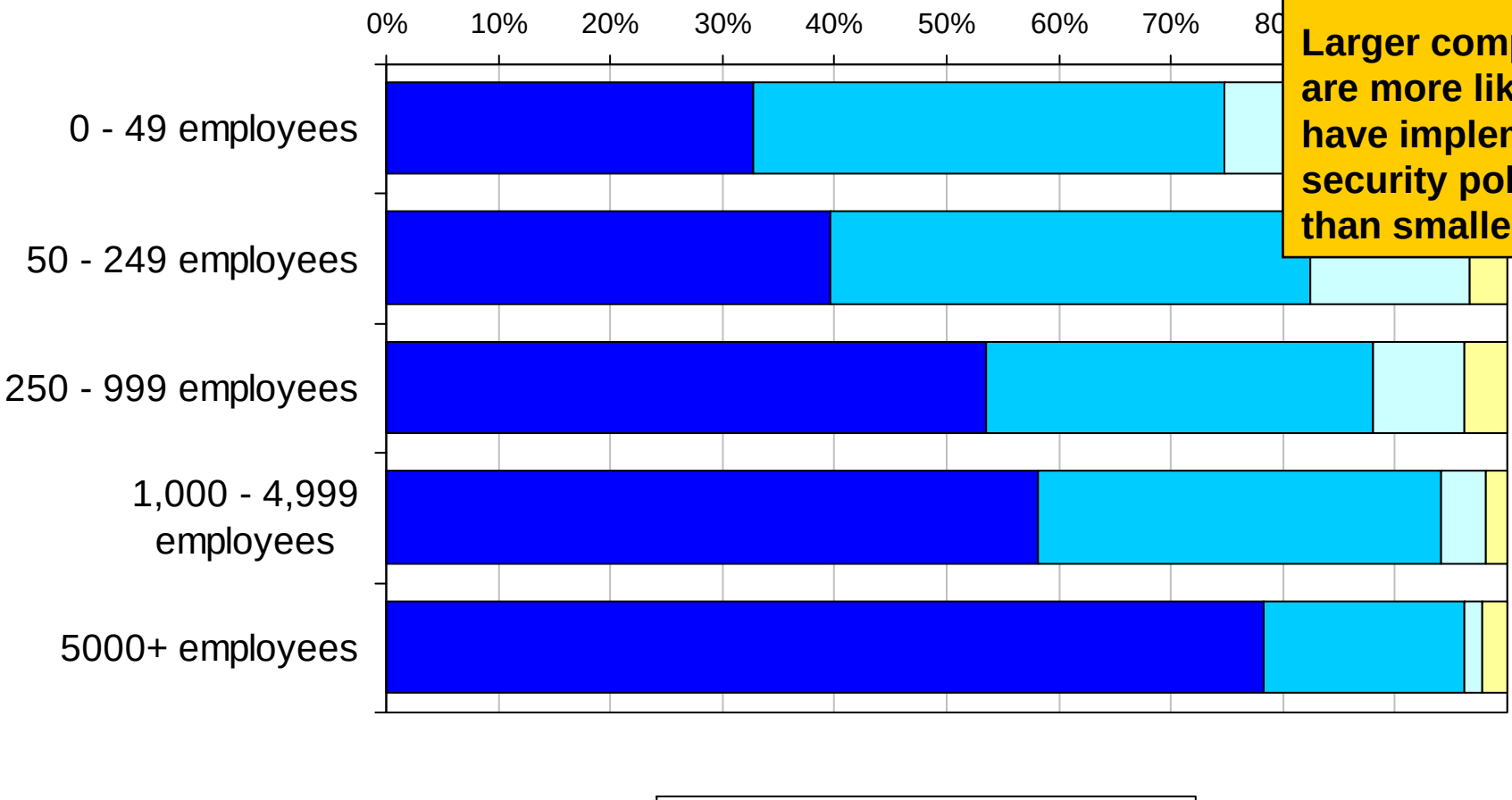
Have your computer systems or web sites been rendered inaccessible due to any of the following?



Observations

Failures due to hardware or software problems appear roughly three times more often than security-related failures. There is the potential that such problems are also security-related.

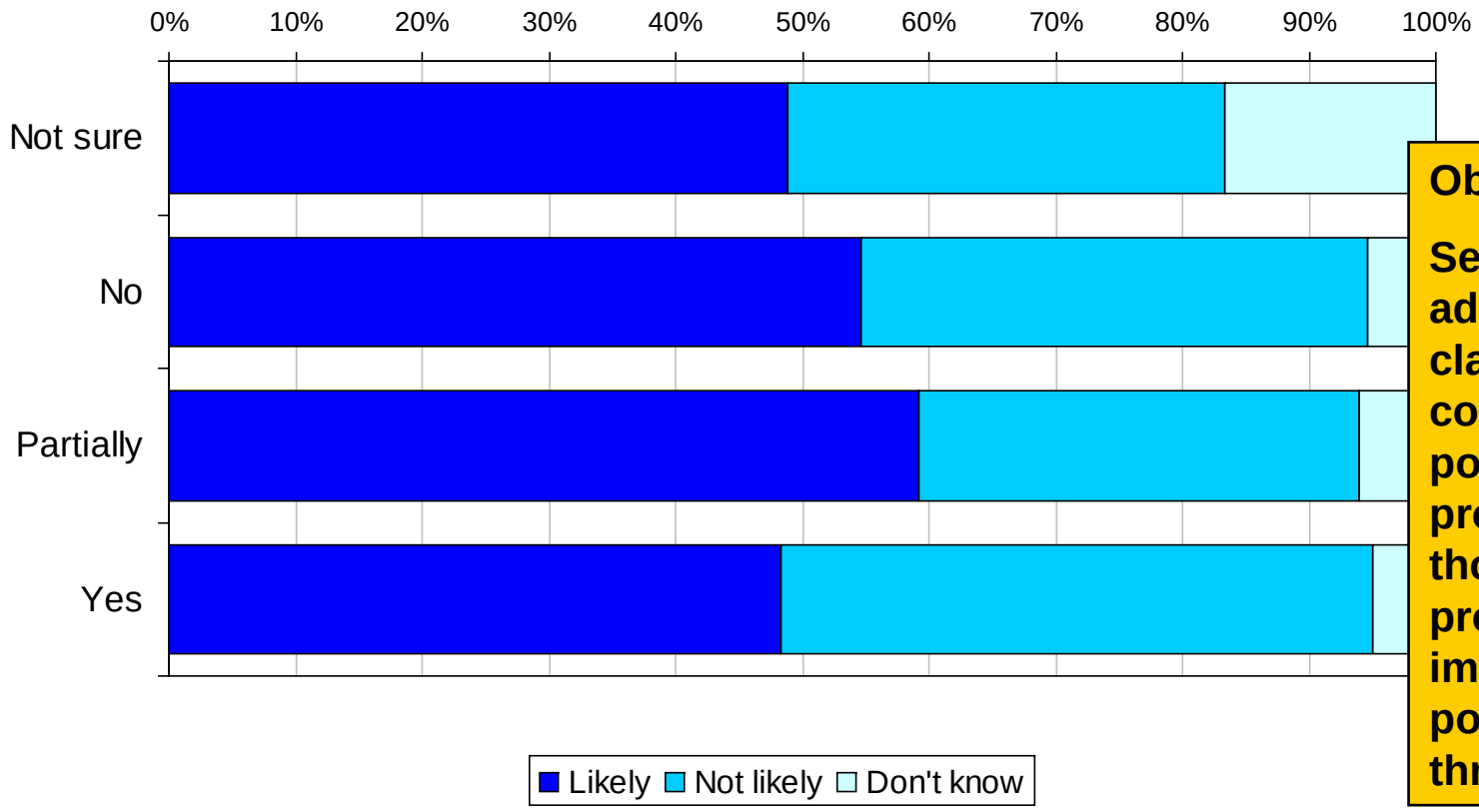
Has your organisation implemented a formal security policy or process?



Observations

Larger companies are more likely to have implemented security policies than smaller ones

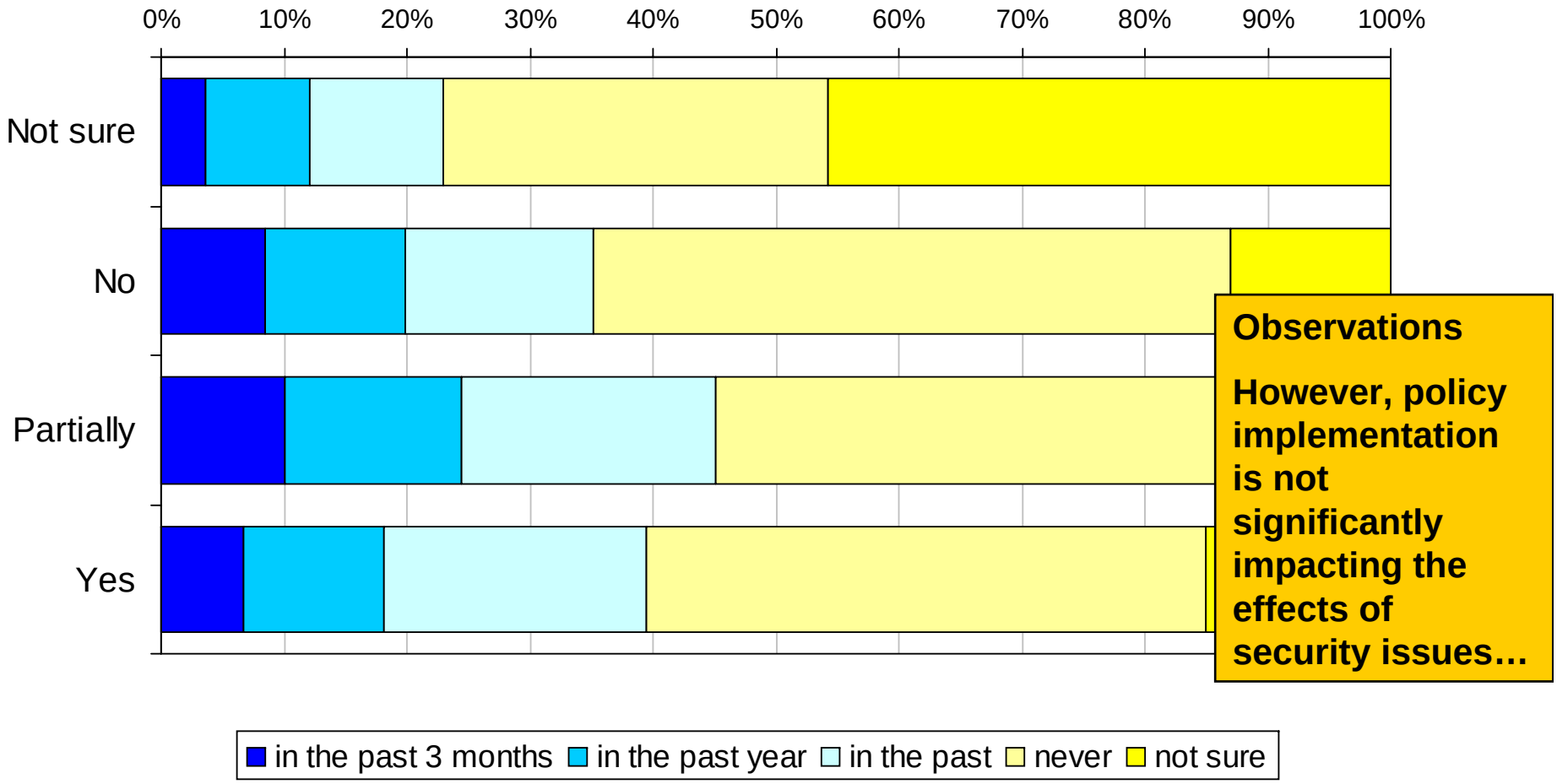
How would you rank the likelihood of a Malware attack occurring in the future?



Observations

Security policy adoption follows a classic curve – companies without policy see fewer problems, while those in the process of implementing a policy feel more threatened

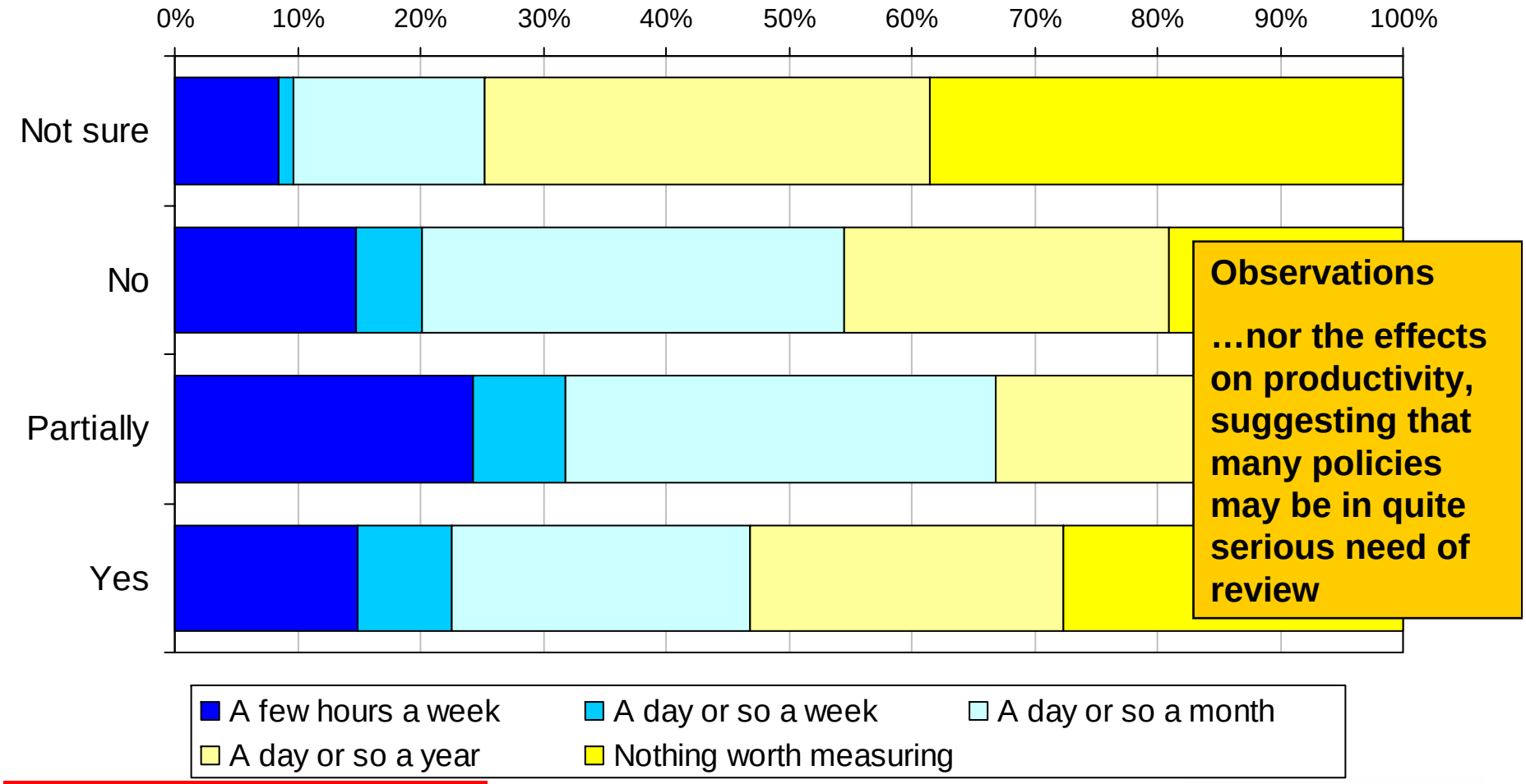
Have your computer systems or web sites been rendered inaccessible due to malicious software?



Observations

However, policy implementation is not significantly impacting the effects of security issues…

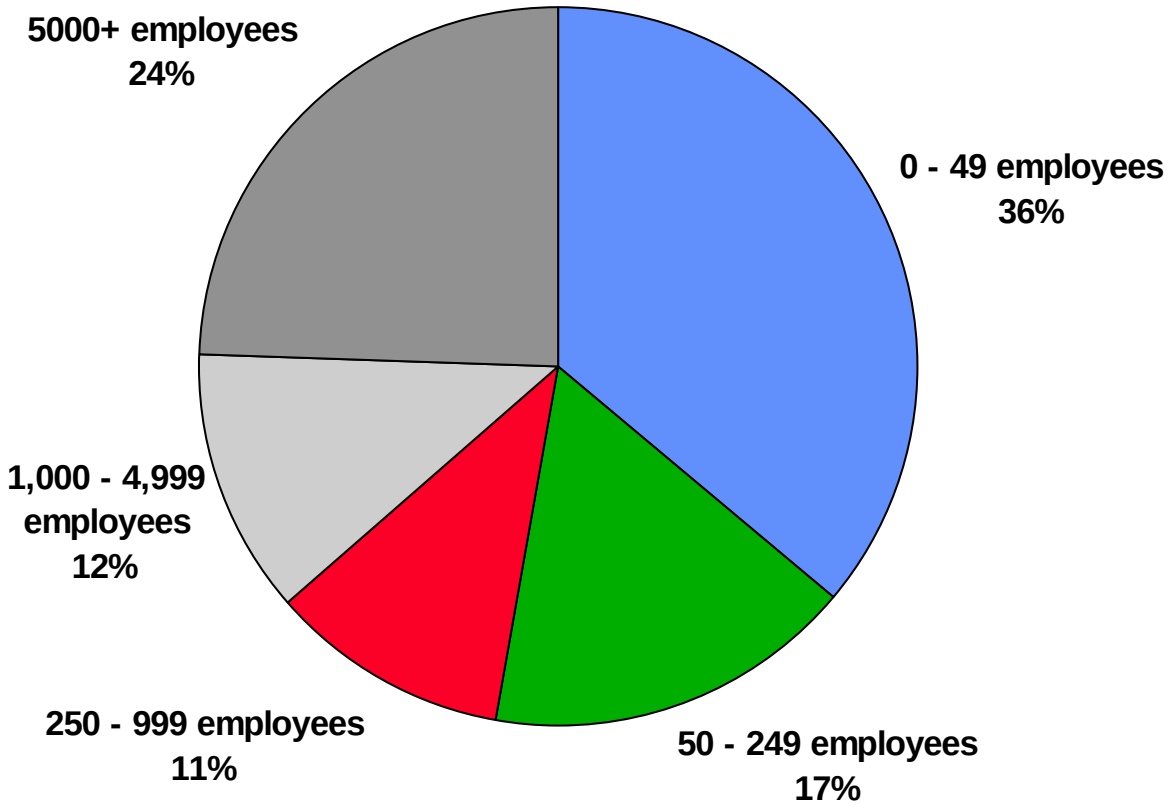
How much time would you consider you waste due to security problems?



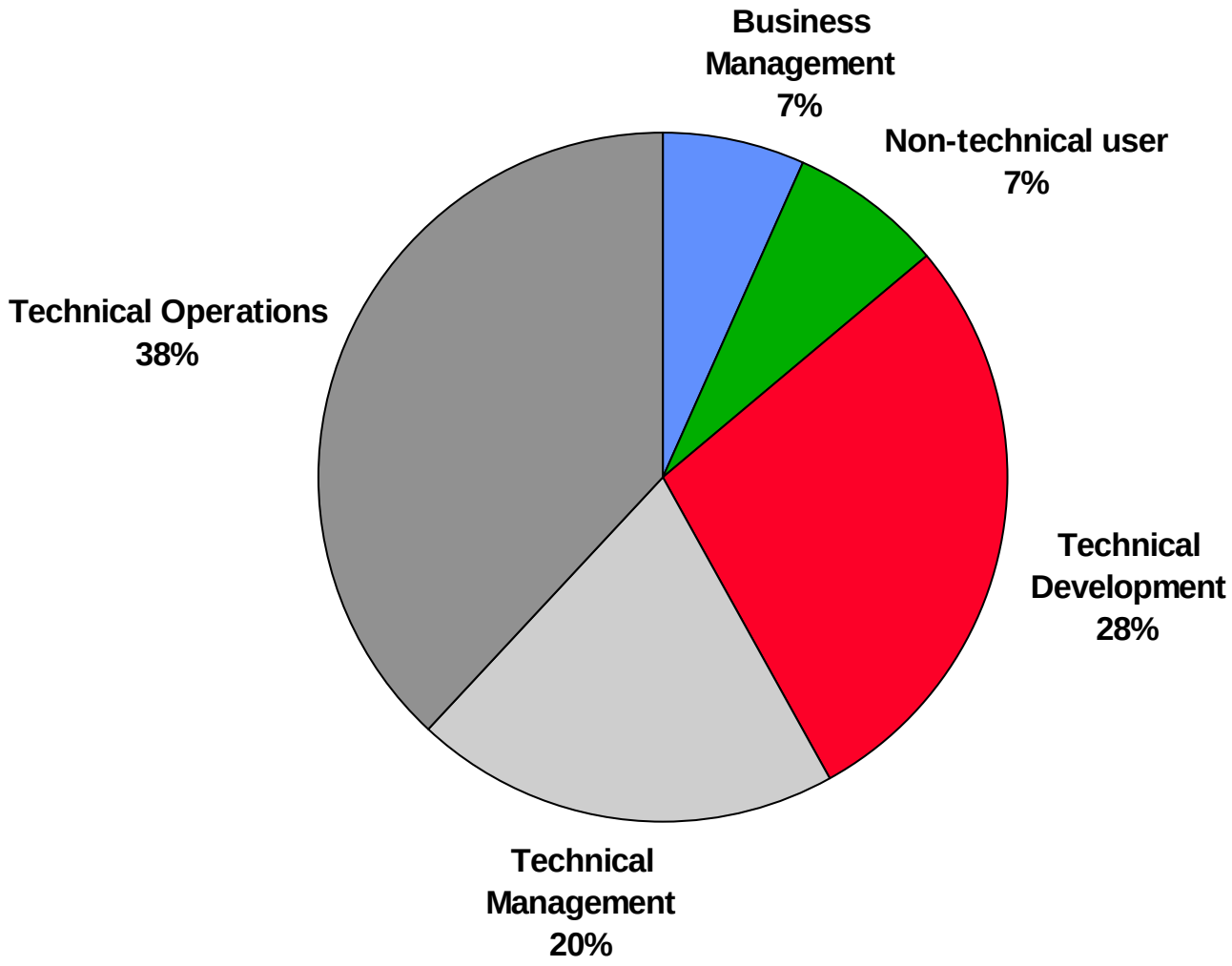
Observations

…nor the effects on productivity, suggesting that many policies may be in quite serious need of review

How large is the organisation you work for?



Which of the following best describes your role in the organisation?



Contacts for feedback and further information

Jon Collins
Quocirca Ltd
+44 1285 771433 (Desk)
jon.collins@quocirca.com

OR

Clive Longbottom
Quocirca Ltd
+44 1189 483360 (Desk)
clive.longbottom@quocirca.com