Jisc Online surveys

Study of Administrator password policy costs Survey 5

Showing 8 of 8 responses

Showing **all** responses

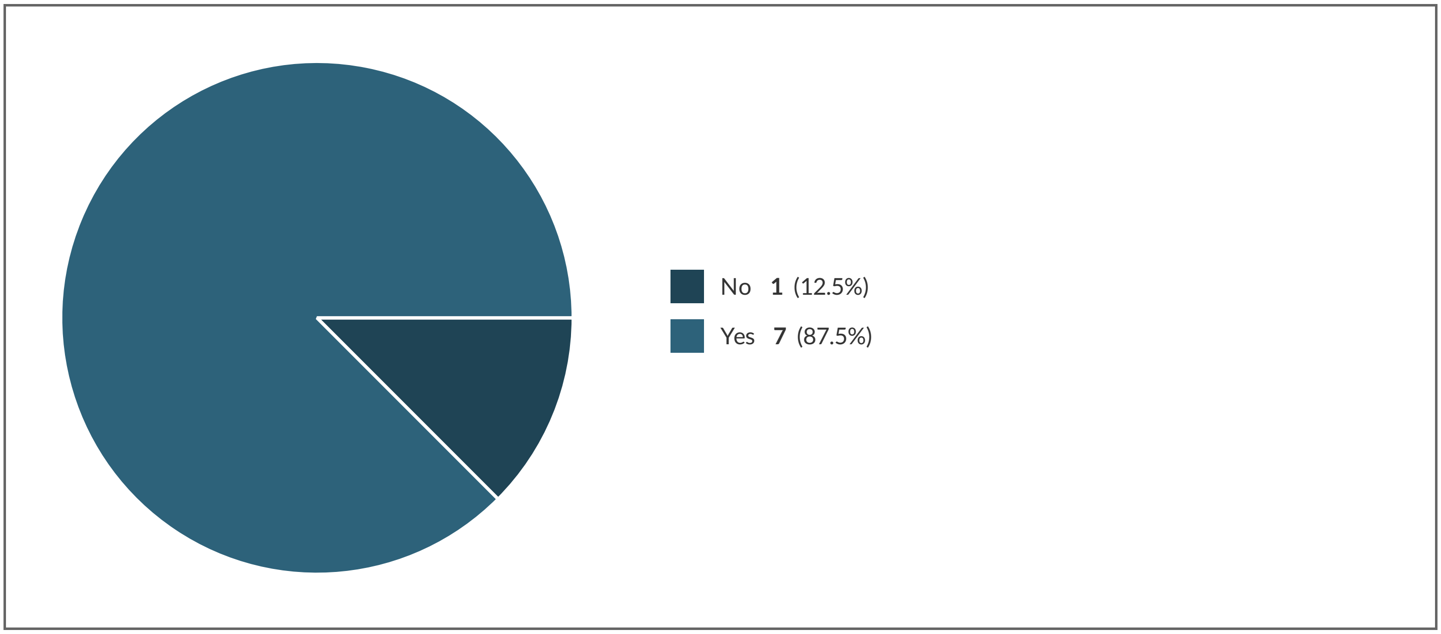
Showing **all** questions

Response rate: 8%

1 Informed consent

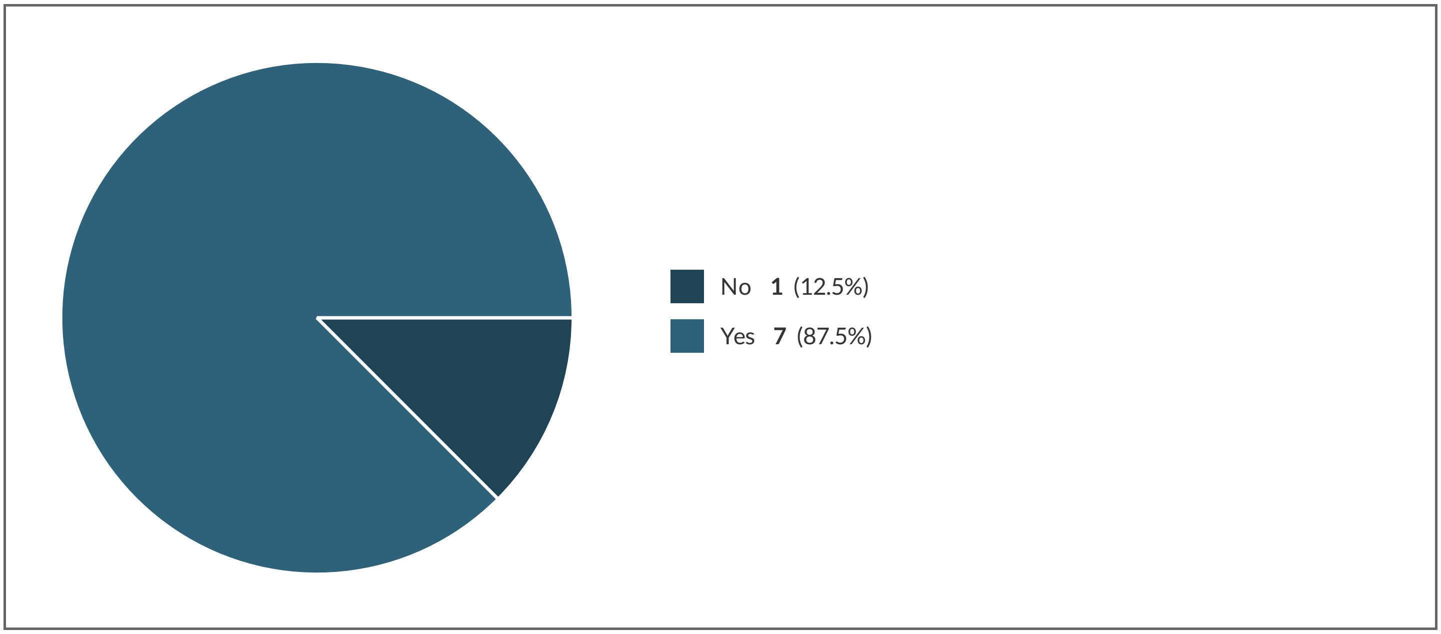
1.1 The purpose and nature of this study has been explained to me.

1.1.a The purpose and nature of this study has been explained to me.



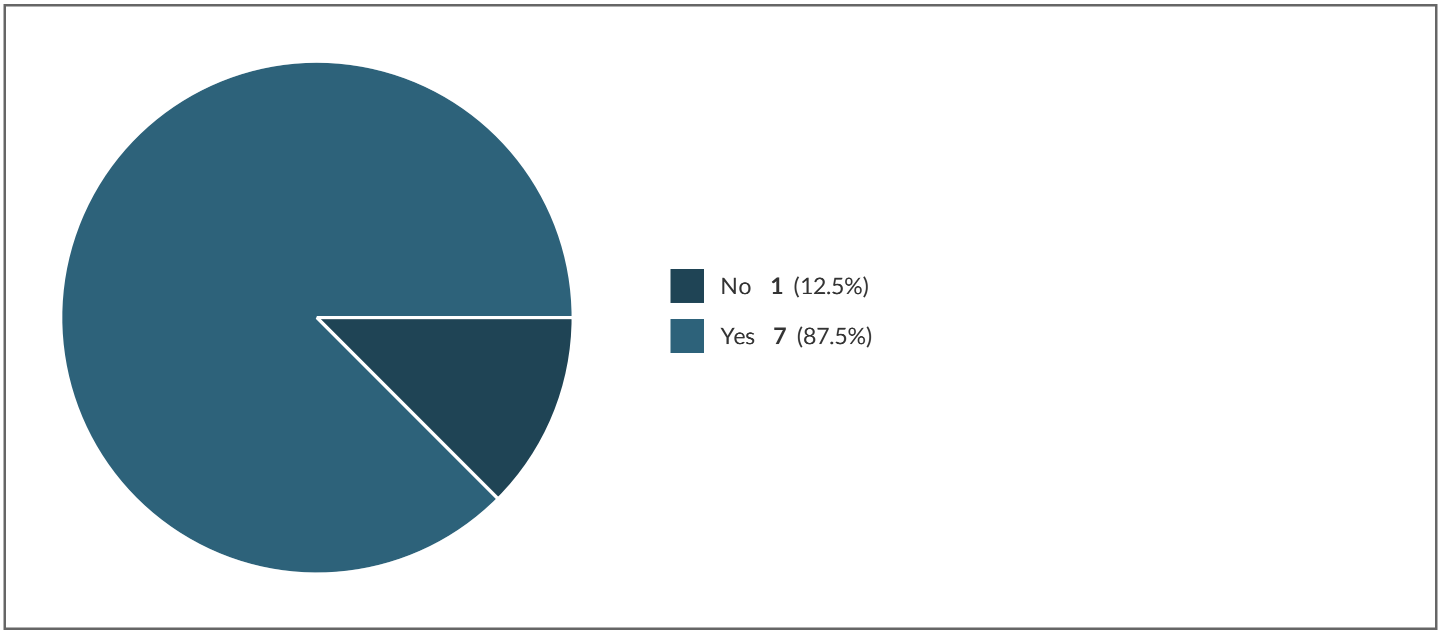
1.2 I am participating voluntarily.

1.2.a I am participating voluntarily.



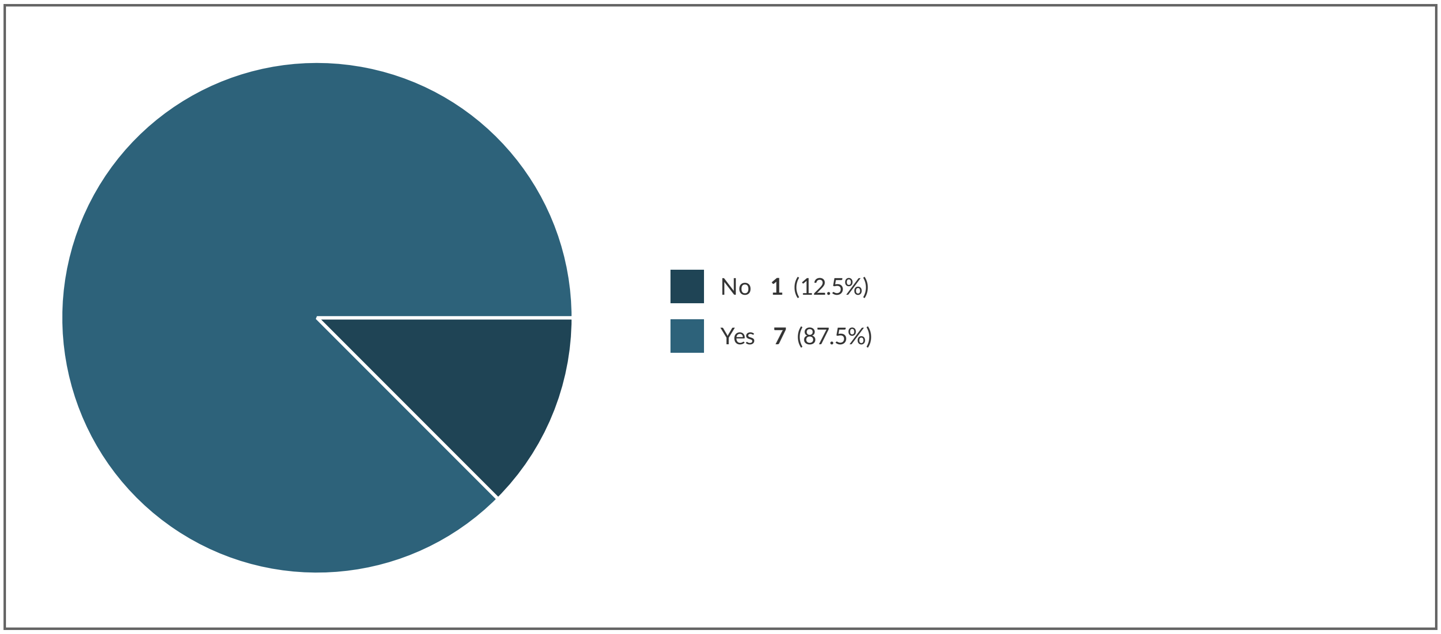
1.3 I understand that I can withdraw from the survey up until it is submitted. I understand that after that point, as the survey is anonymous, it will not be possible to identify and remove the data.

1.3.a I understand that I can withdraw from the survey up until it is submitted. I understand that after that point, as the survey is anonymous, it will not be possible to identify and remove the data.



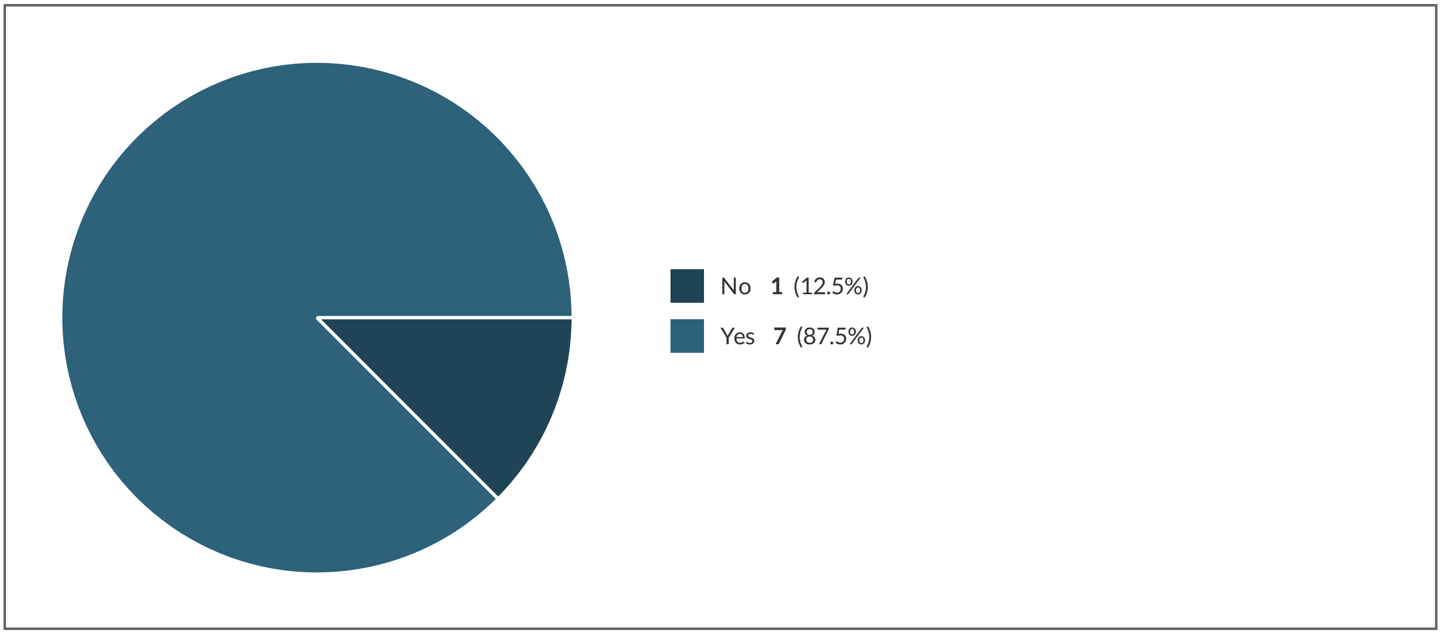
1.4 I understand the limits of confidentiality as described in the information sheet.

1.4.a I understand the limits of confidentiality as described in the information sheet.

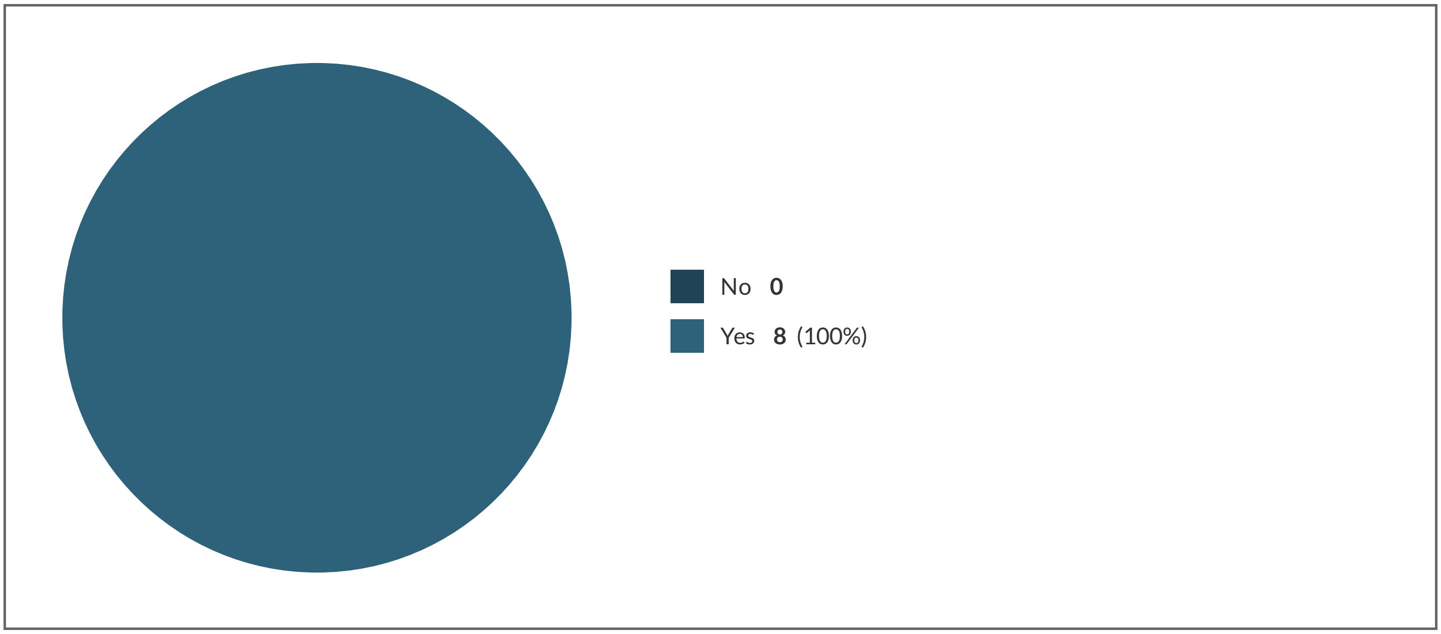


1.5 I understand that my anonymous responses may be used in future research projects and the data from this study may be deposited in an archive if I give permission here:

1.5.a I understand that my anonymous responses may be used in future research projects and the data from this study may be deposited in an archive if I give permission here:



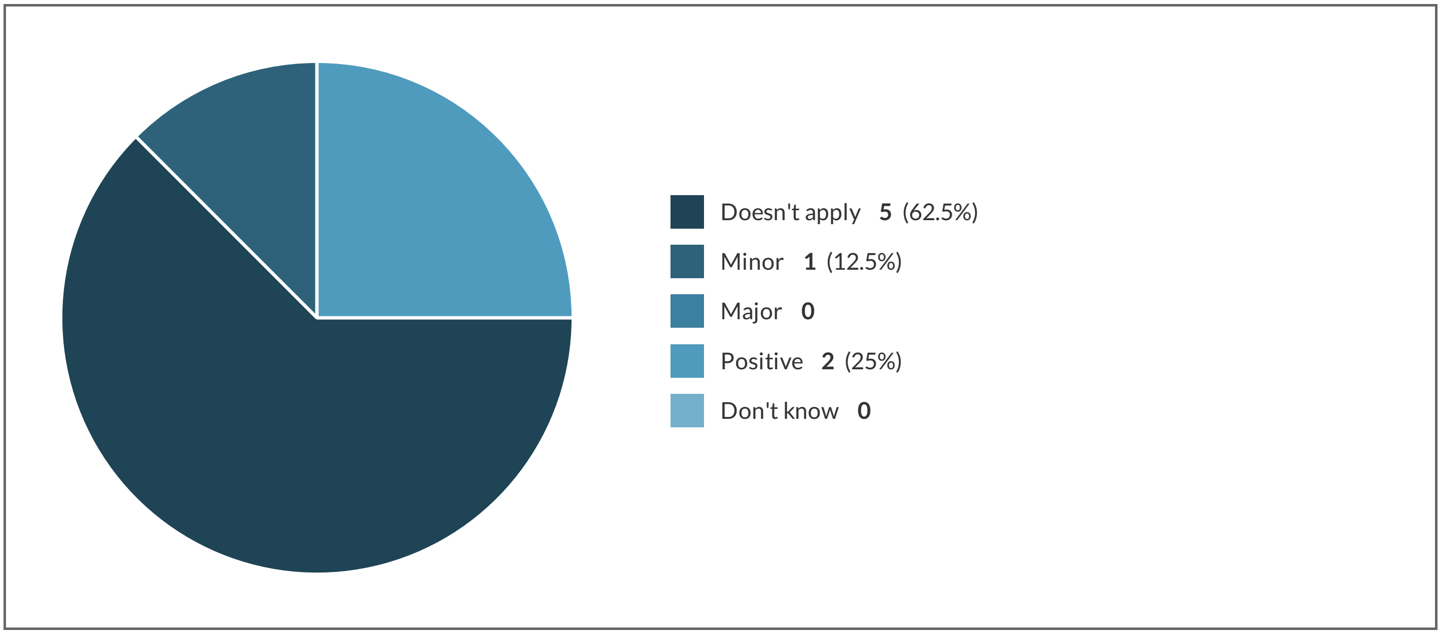
2 I consent to participate in this survey:



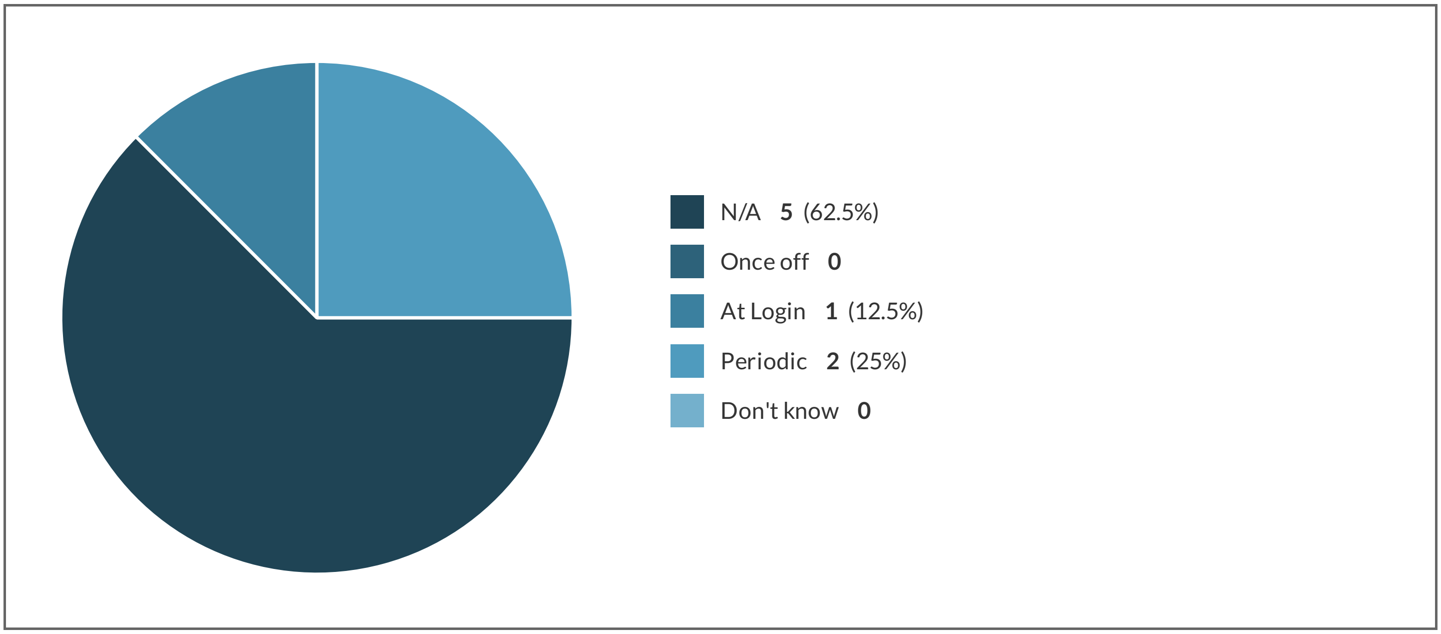
3 Password files should be encrypted

3.1 Increased help desk/user support time

3.1.a Increased help desk/user support time - Severity of Cost

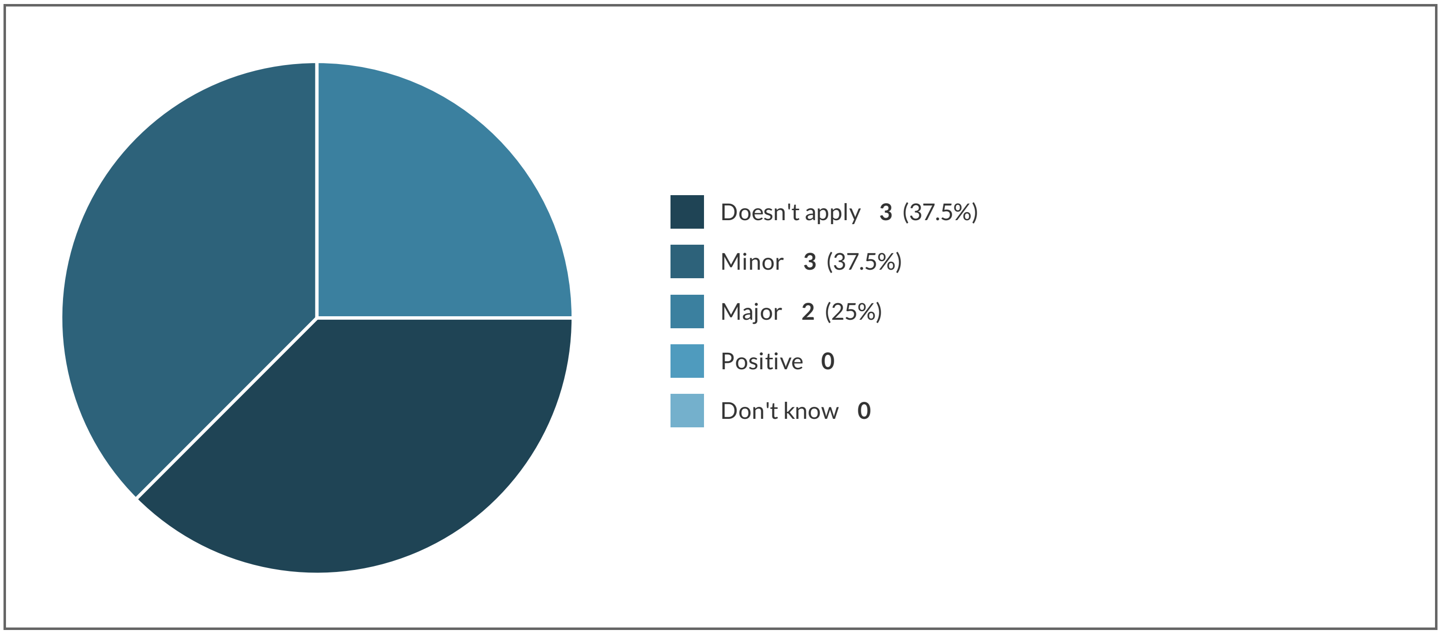


3.1.b Increased help desk/user support time - Frequency Cost is Experienced

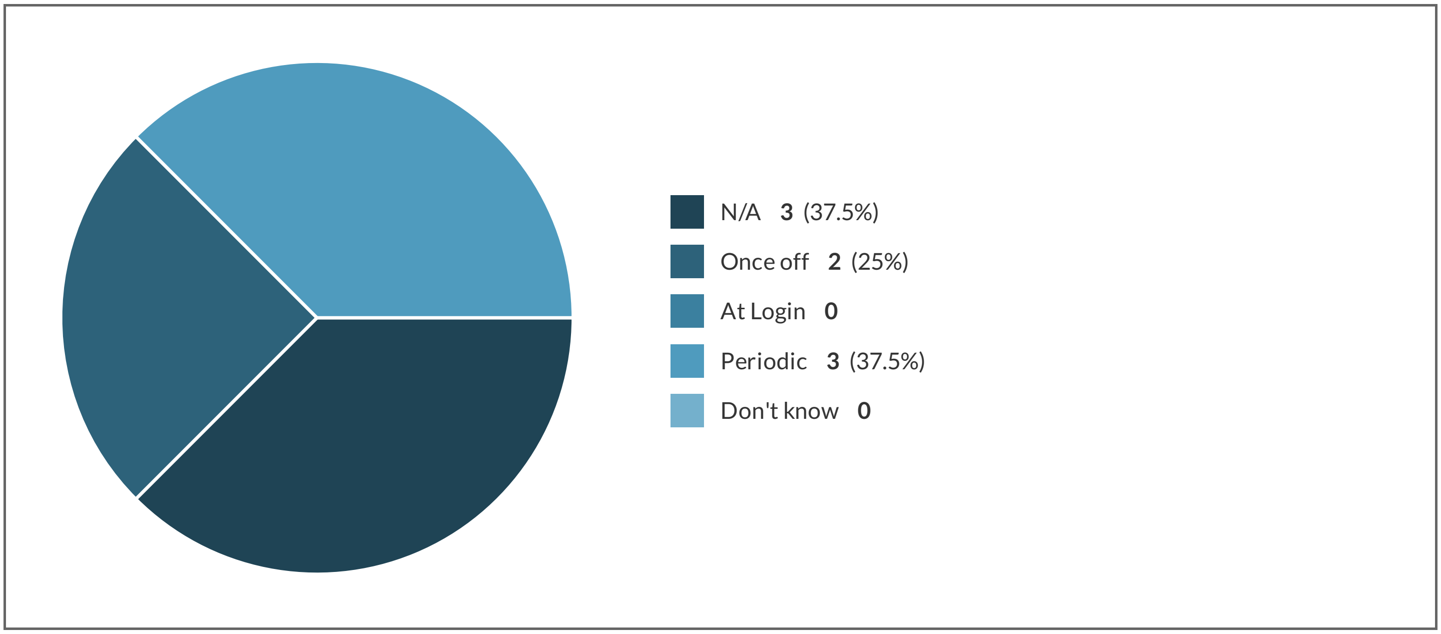


3.2 User education required

3.2.a User education required - Severity of Cost

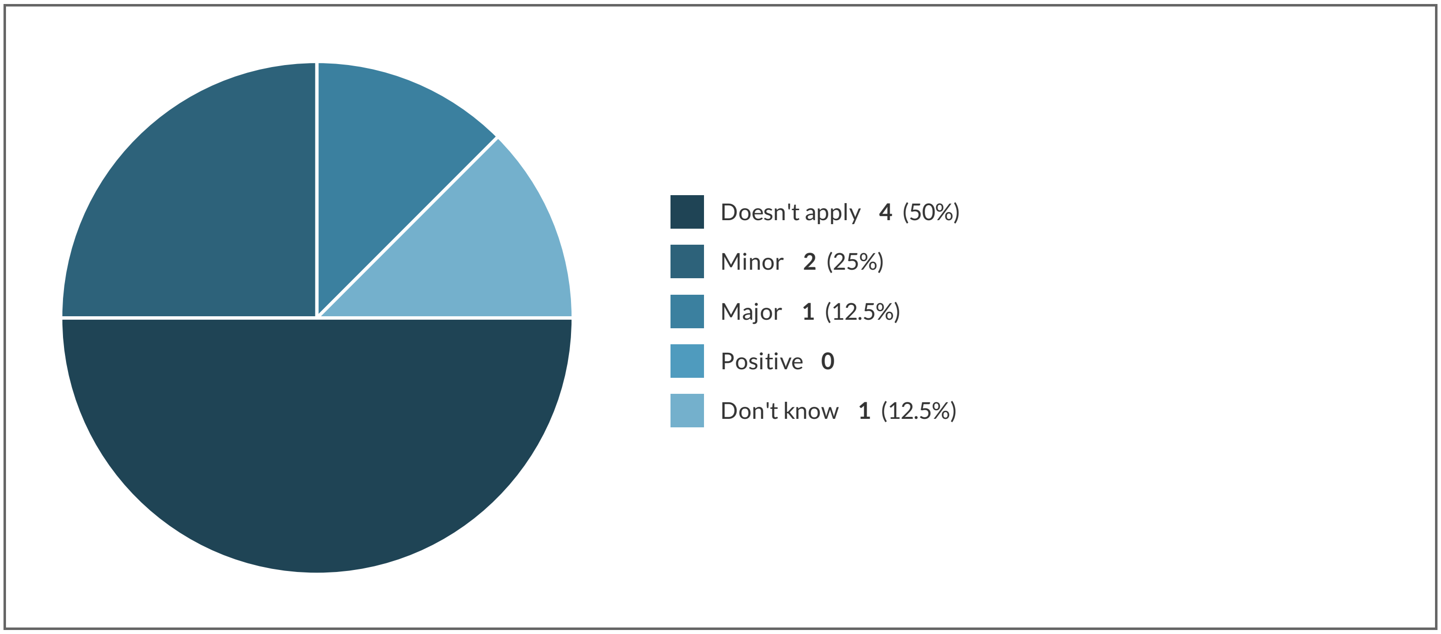


3.2.b User education required - Frequency Cost is Experienced

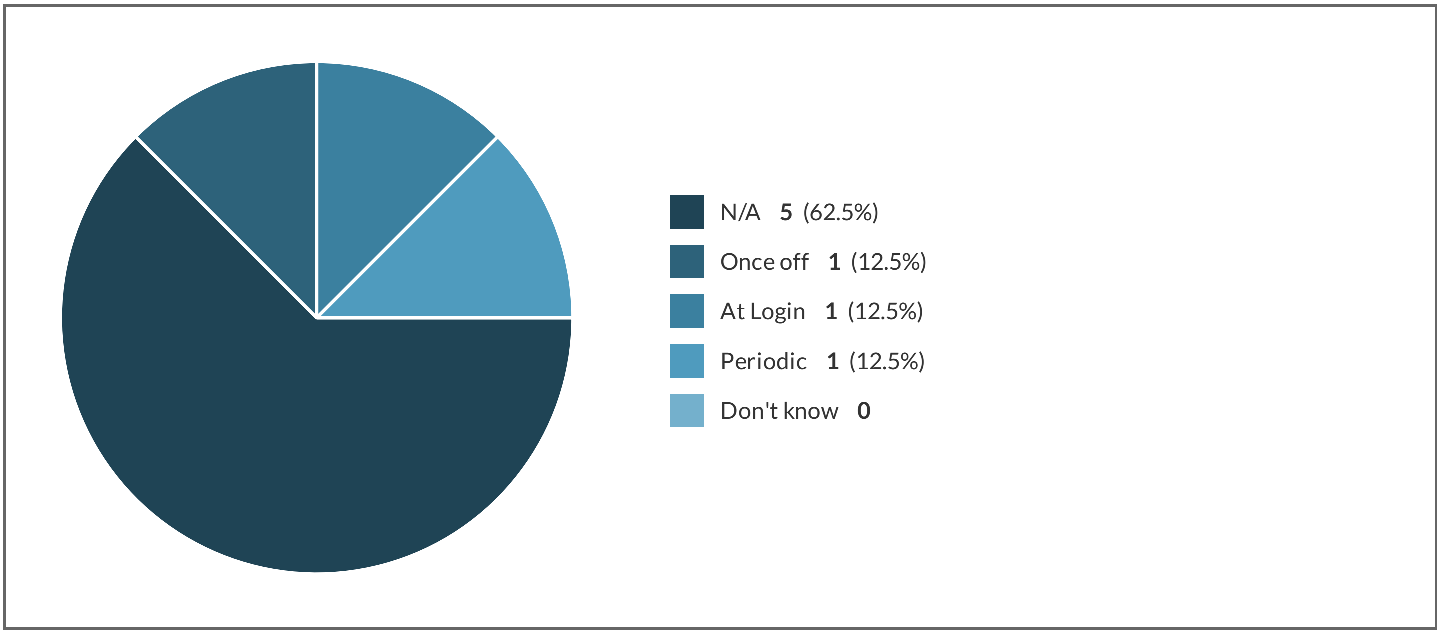


3.3 Organization needs extra resources

3.3.a Organization needs extra resources - Severity of Cost

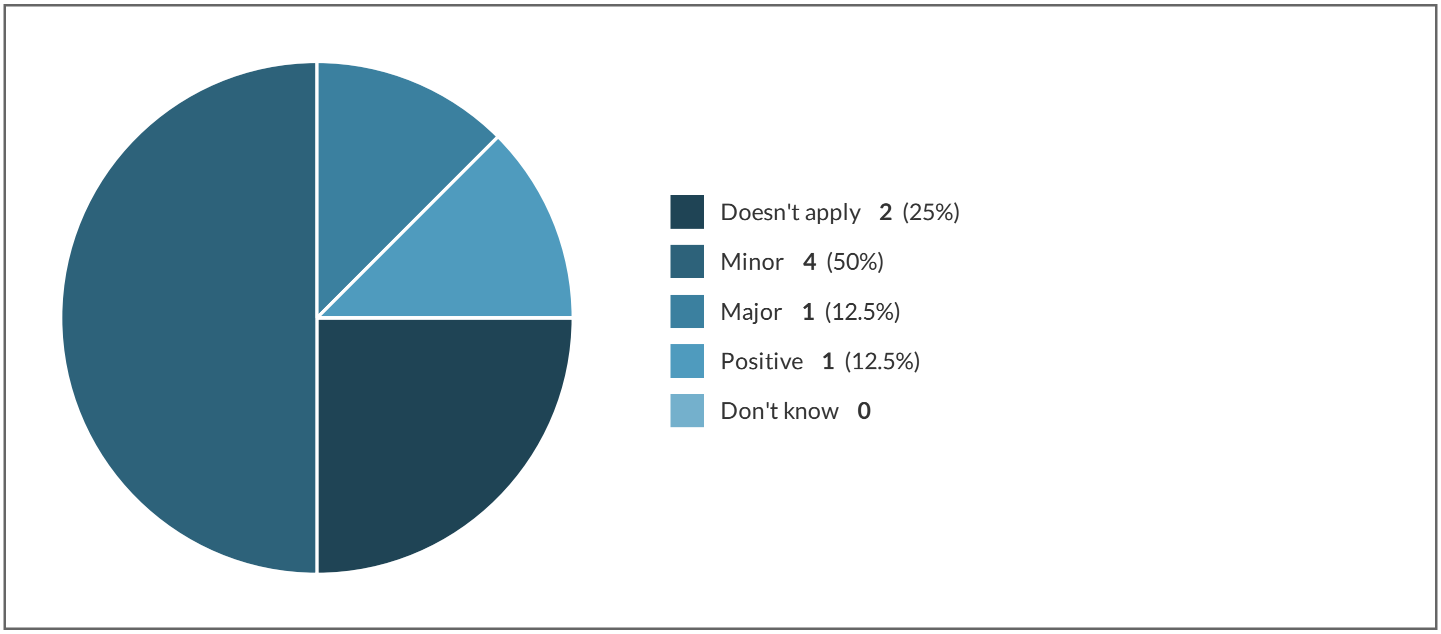


3.3.b Organization needs extra resources - Frequency Cost is Experienced

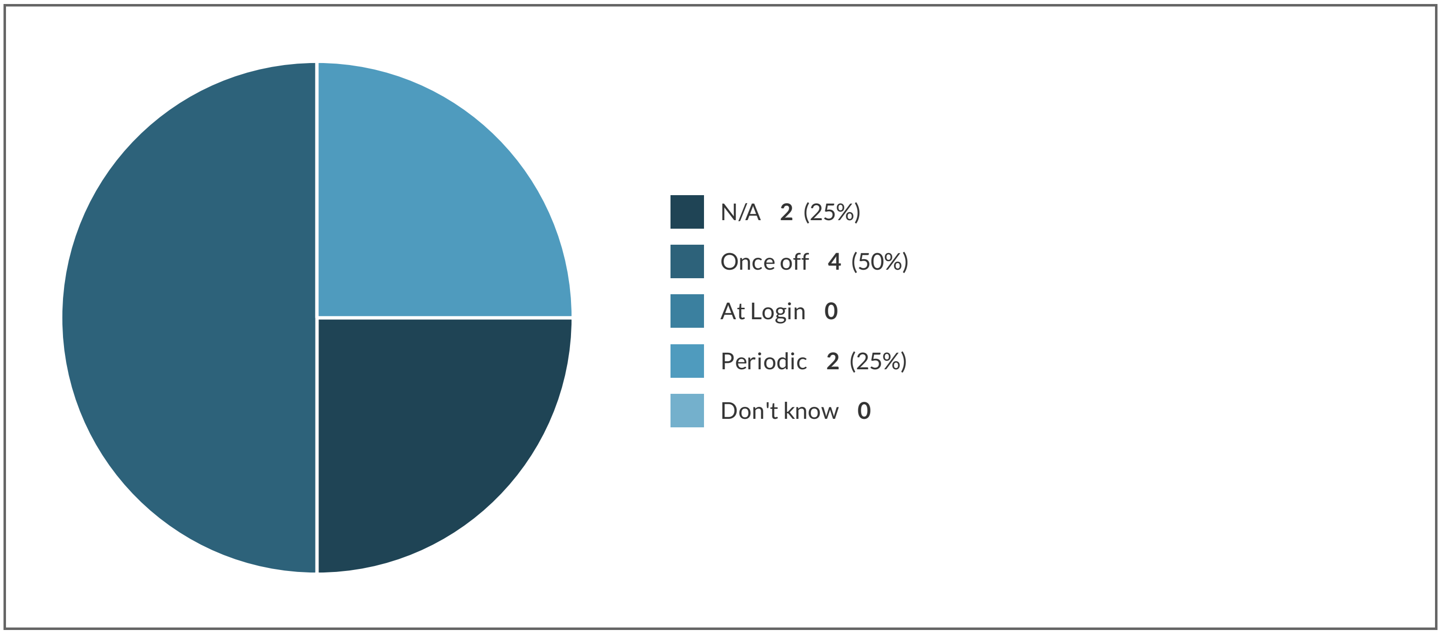


3.4 Takes organization time to implement

3.4.a Takes organization time to implement - Severity of Cost

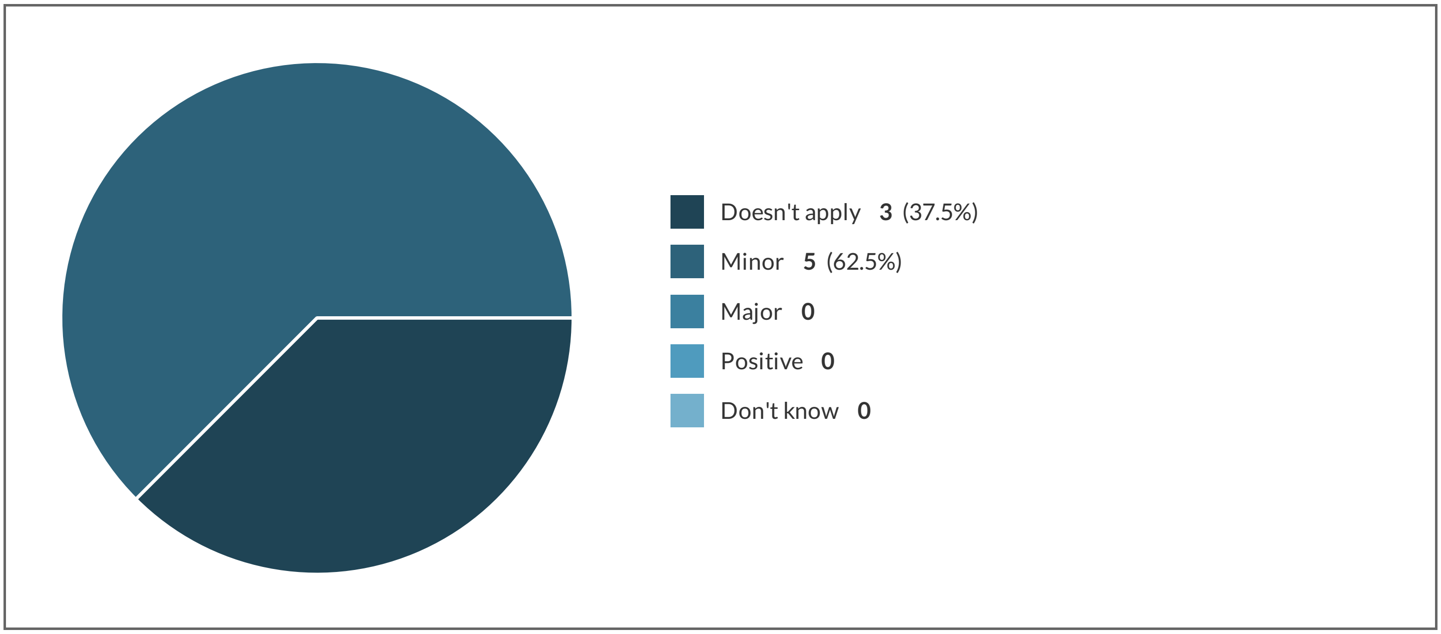


3.4.b Takes organization time to implement - Frequency Cost is Experienced

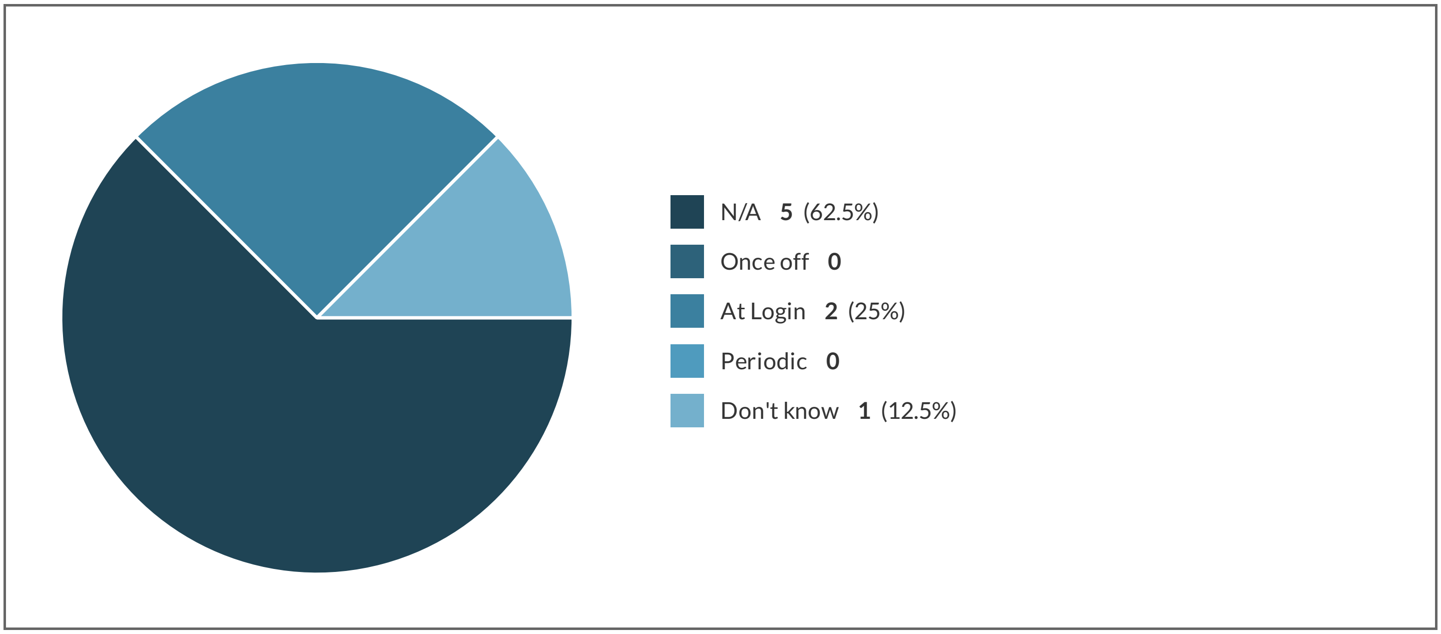


3.5 Increases the organization's computing power needed

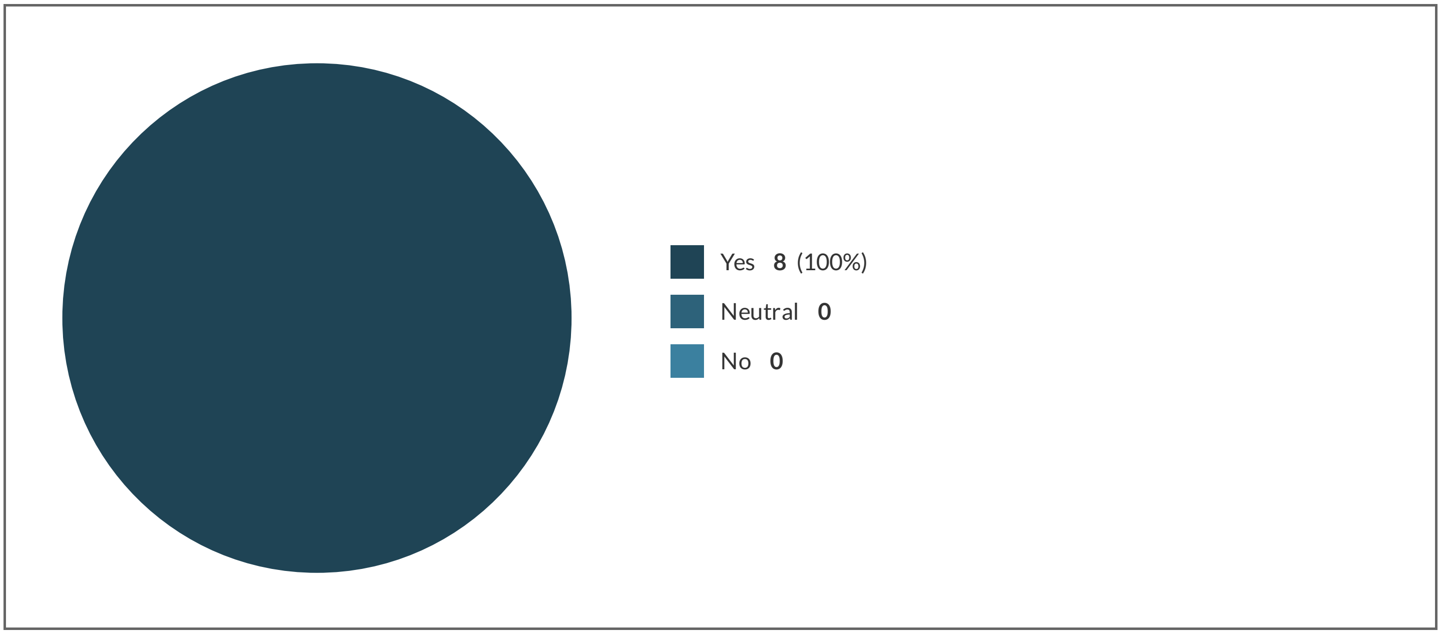
3.5.a Increases the organization's computing power needed - Severity of Cost



3.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



3.a Do you approve of this advice?



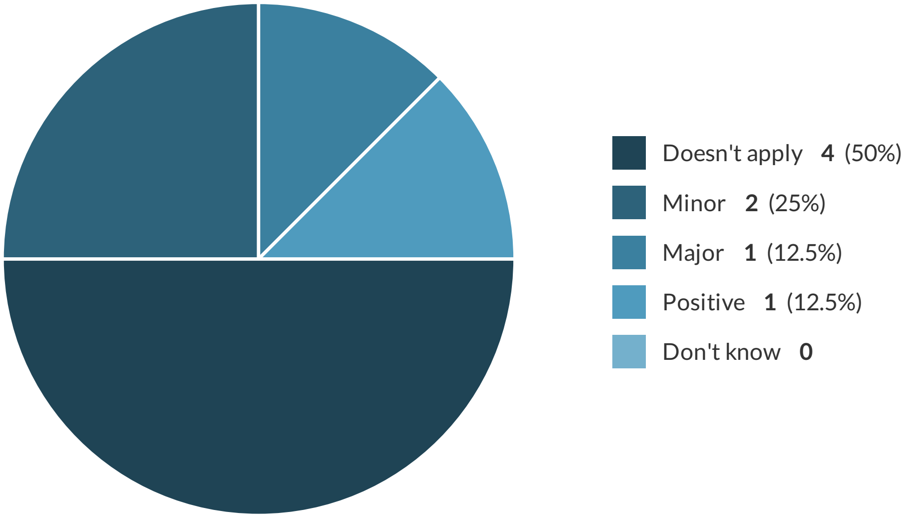
3.b Comments

Showing all 5 responses	
most central password files should always be encrypted and done on creation. Users don't necessarly follow this procedure for their own files	634211-634202-66098698
Unclear what “resources” might be	634211-634202-66532254
As this is already the default in every sensible system, I don't consider this to have any cost.	634211-634202-66532992
It's common practice to ensure password files are encrypted.. To me this is a no brainer	634211-634202-66754804
So this question slightly confused me as to what you were referring to with "Password Files" if you mean files that require a password, yeah certainly. If you mean files containing passwords those really shouldn't exist if at all possible and definitely should be encrypted	634211-634202-66754952

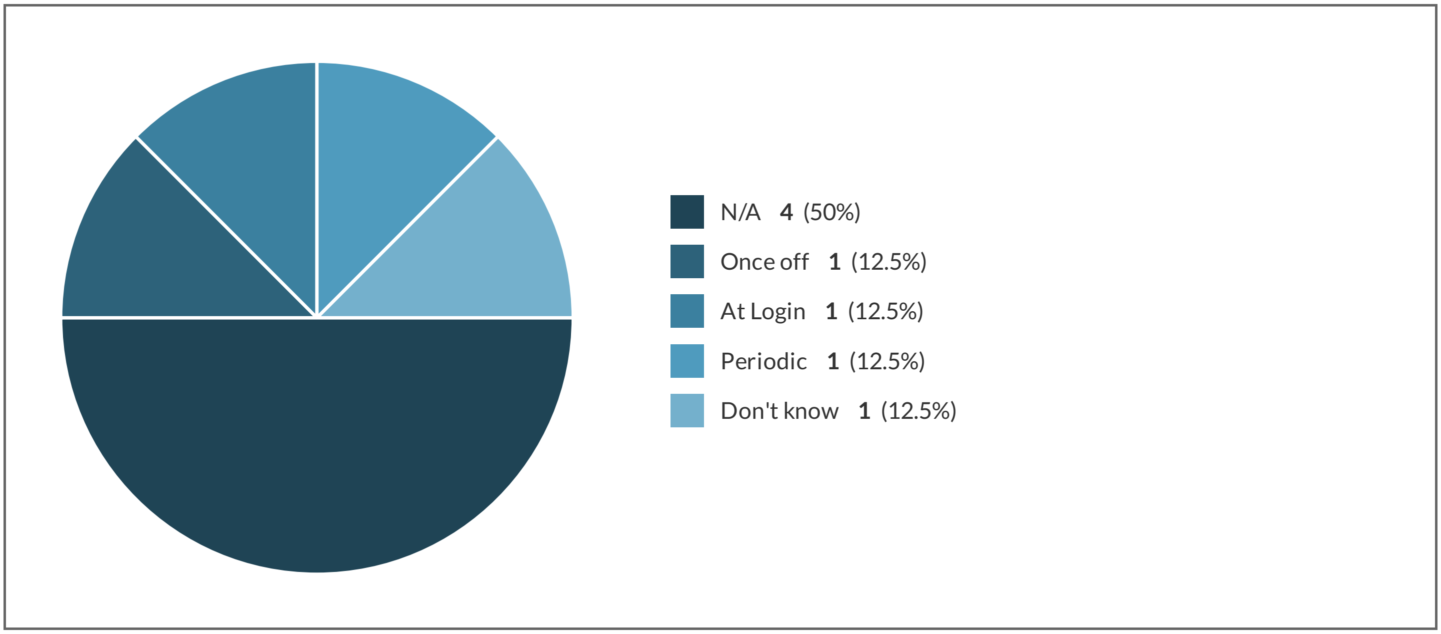
4 Historical passwords should be stored to prevent password reuse

4.1 Increased help desk/user support time

4.1.a Increased help desk/user support time - Severity of Cost

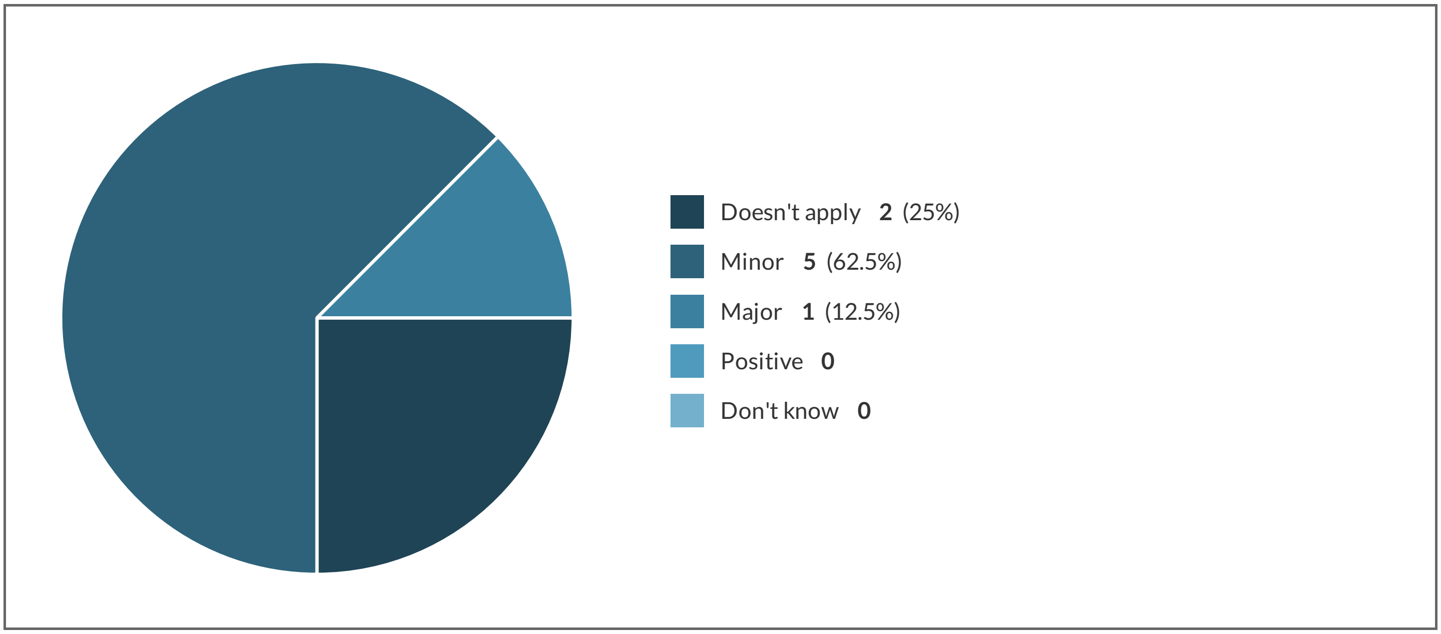


4.1.b Increased help desk/user support time - Frequency Cost is Experienced

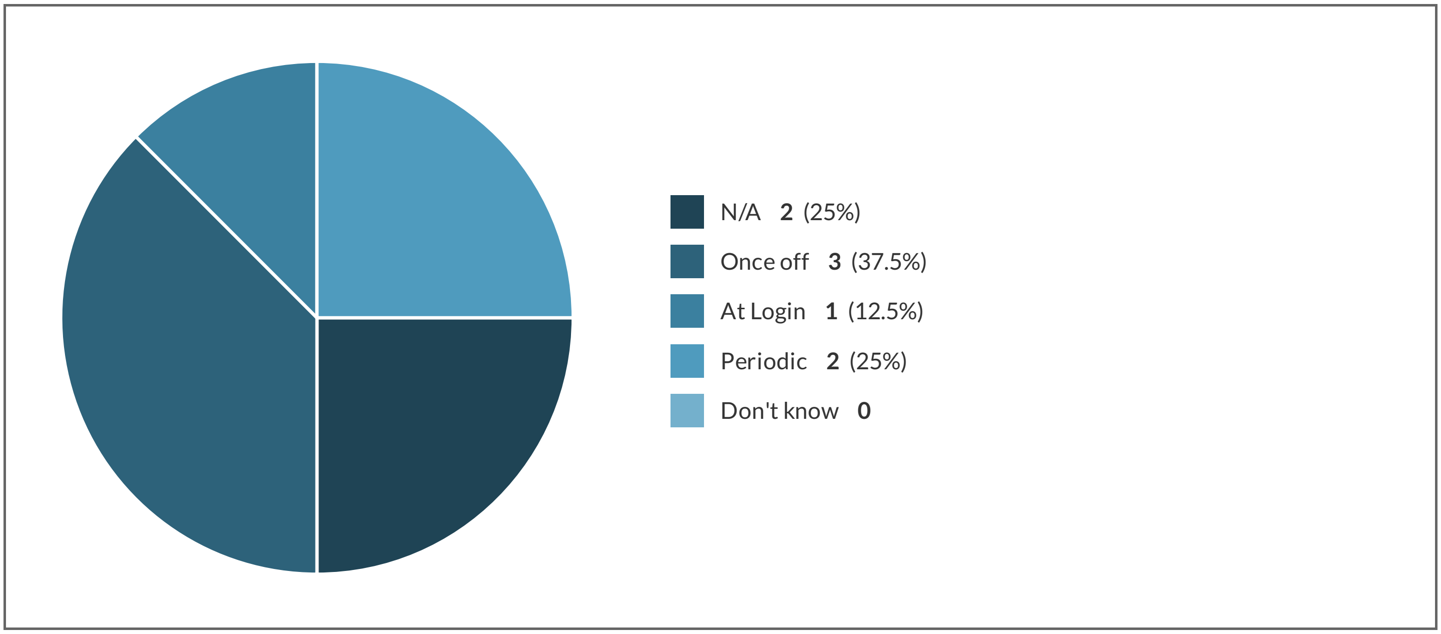


4.2 User education required

4.2.a User education required - Severity of Cost

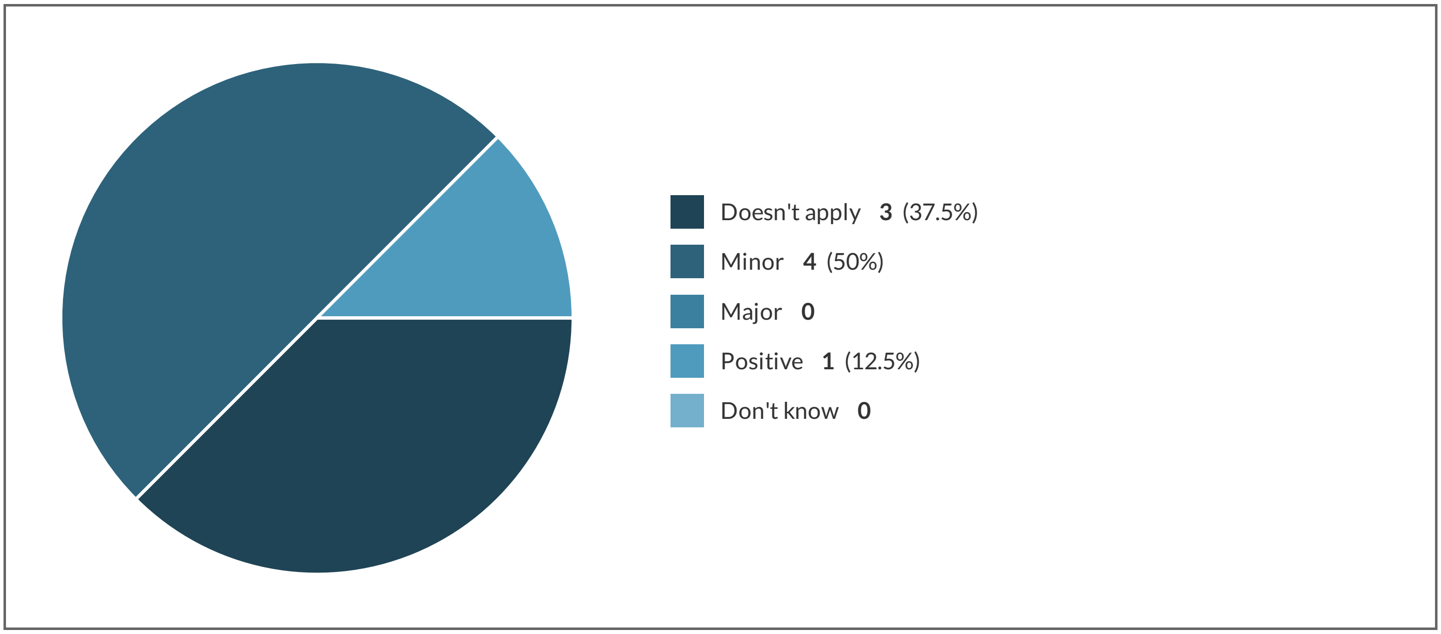


4.2.b User education required - Frequency Cost is Experienced

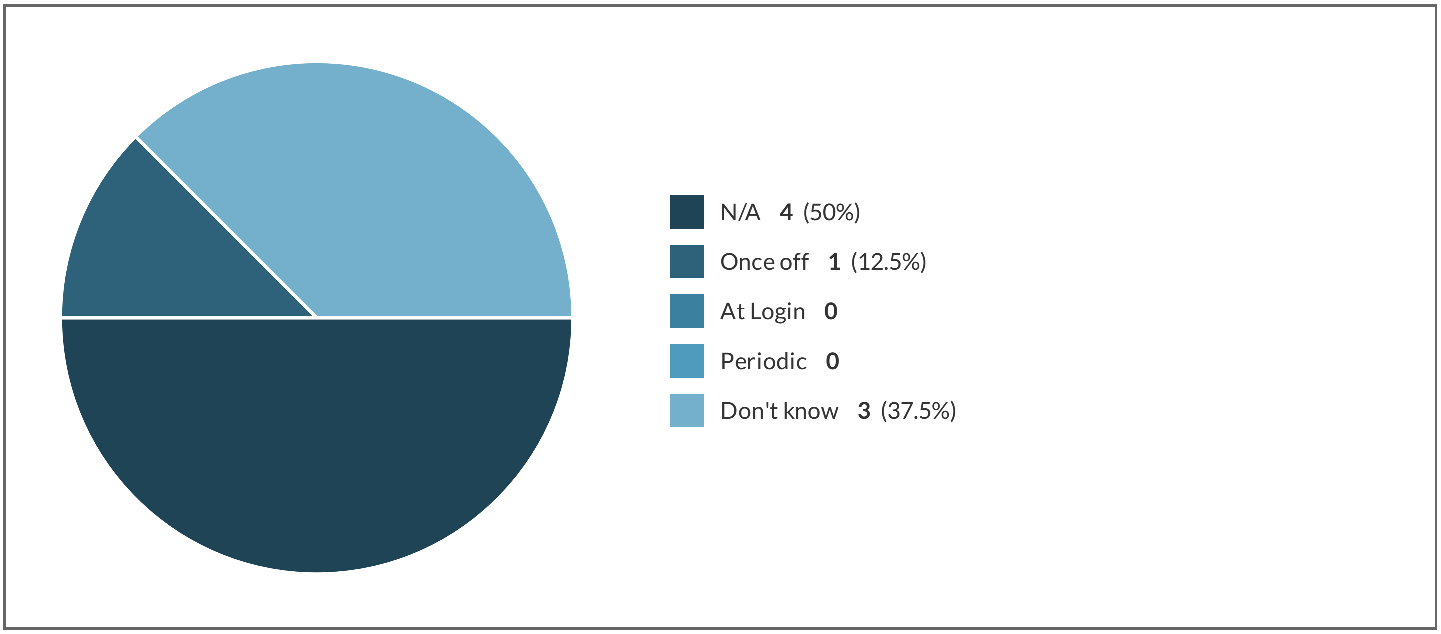


4.3 Organization needs extra resources

4.3.a Organization needs extra resources - Severity of Cost

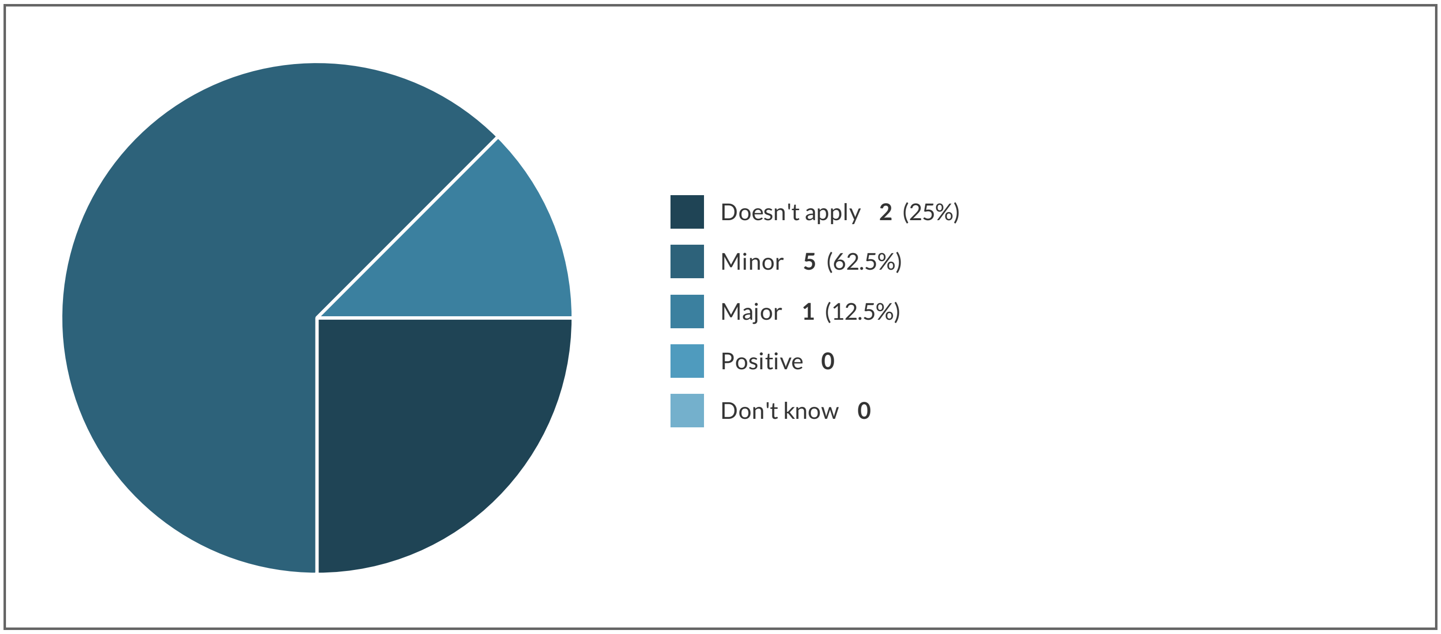


4.3.b Organization needs extra resources - Frequency Cost is Experienced

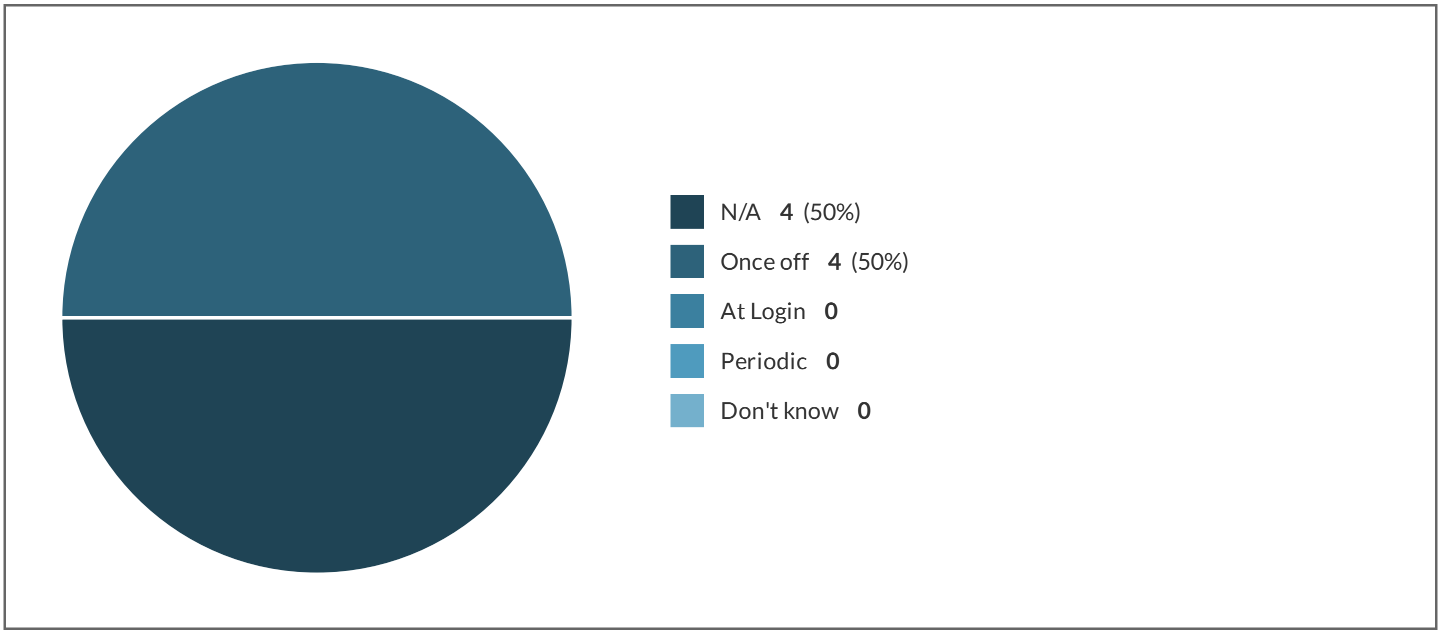


4.4 Takes organization time to implement

4.4.a Takes organization time to implement - Severity of Cost

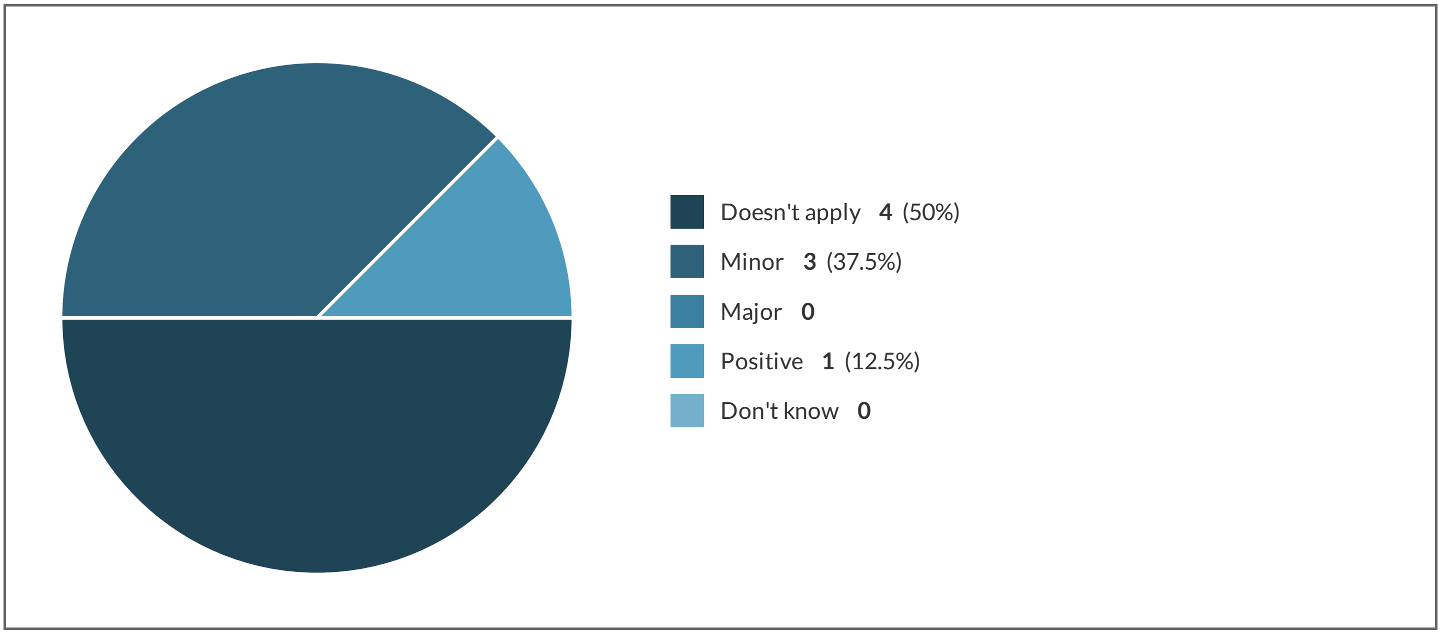


4.4.b Takes organization time to implement - Frequency Cost is Experienced

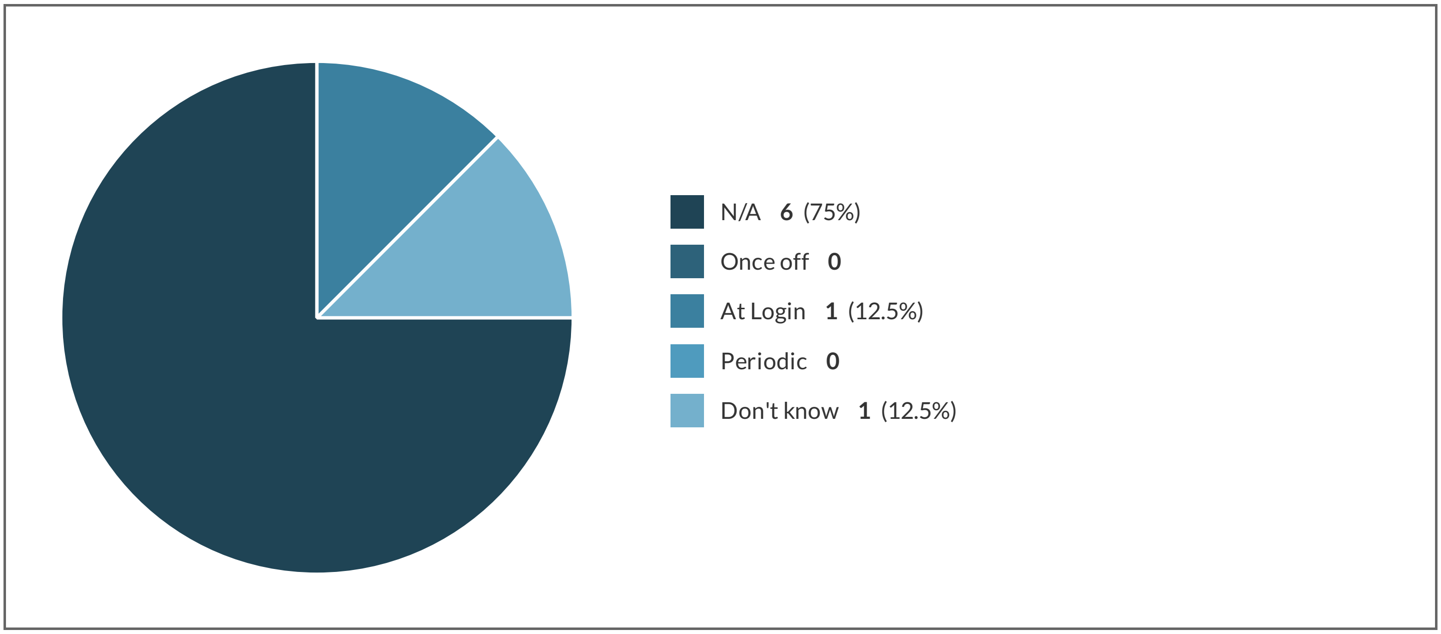


4.5 Increases the organization's computing power needed

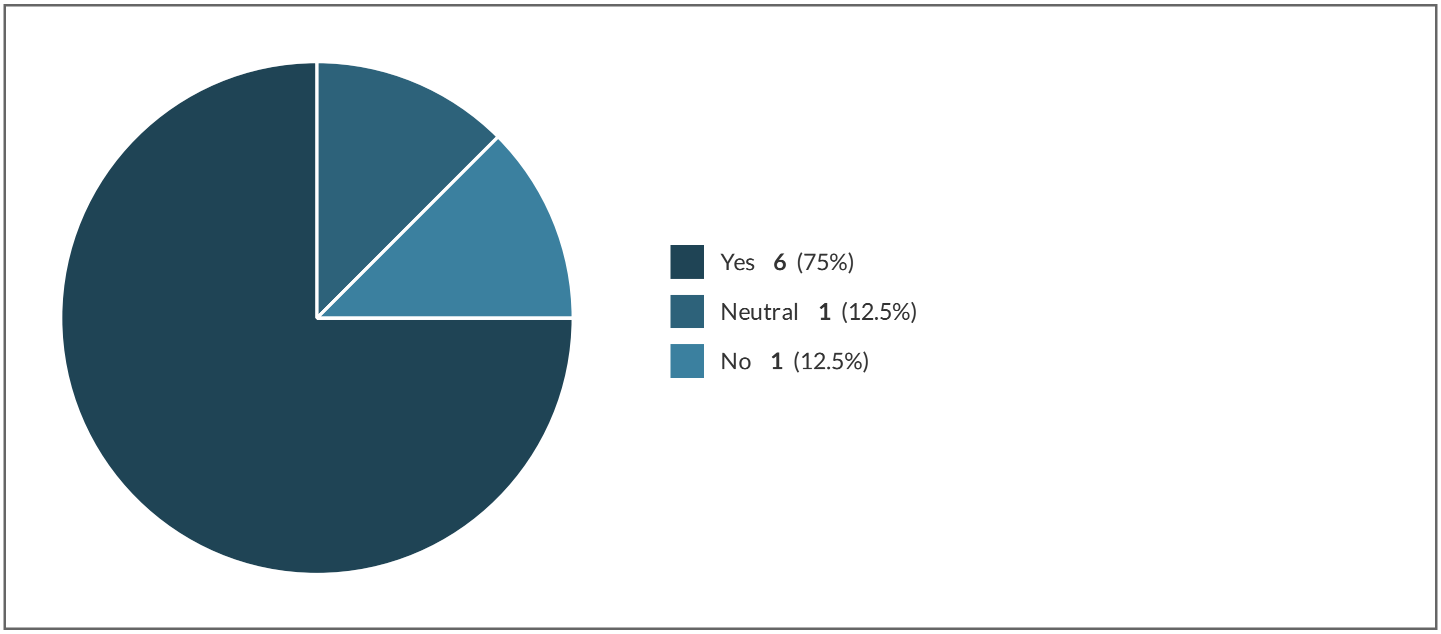
4.5.a Increases the organization's computing power needed - Severity of Cost



4.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



4.a Do you approve of this advice?



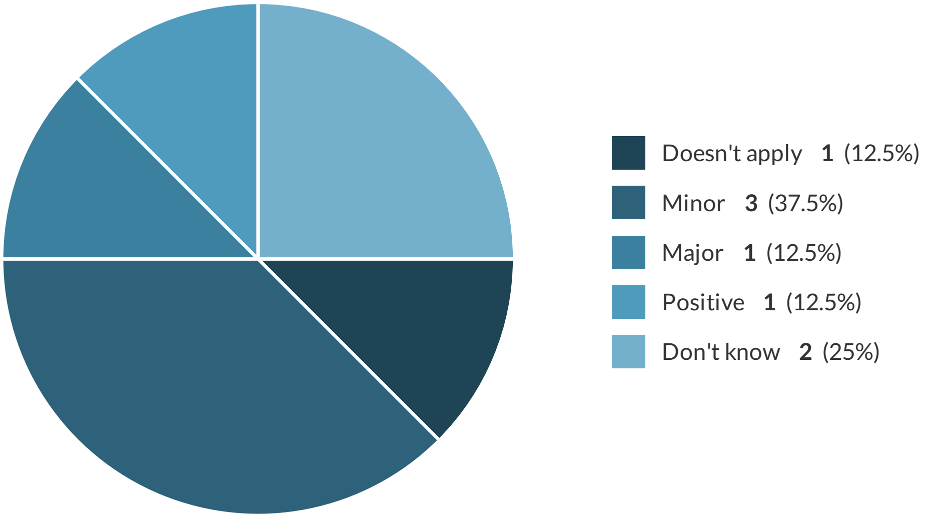
4.b Comments

Showing all 5 responses	
Matters when passwords are changed which is occasionally rather than periodic	634211-634202-66532254
Hashes should be stored, not the actual passwords	634211-634202-66532992
Storing used passwords is policy in the companys I've worked for but I can understand frustration from end users as there is only a finite amount of passwords one can remember	634211-634202-66754804
Always a good idea, people will tend to use their old password with an incremented number on the end though. Of course these passwords should be hashed and salted while being stored too.	634211-634202-66754952
If you require too many new passwords people are inclined to use easier or formula passwords	634211-634202-66871889

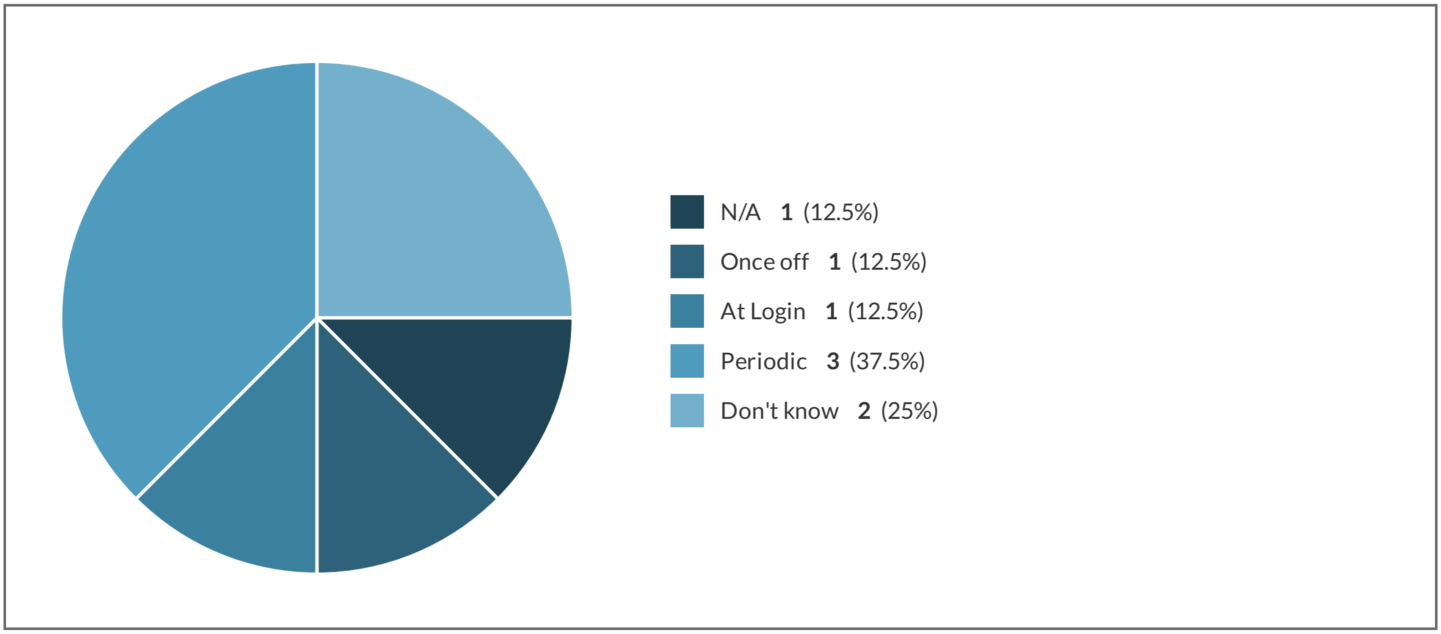
5 All default passwords should be changed

5.1 Increased help desk/user support time

5.1.a Increased help desk/user support time - Severity of Cost

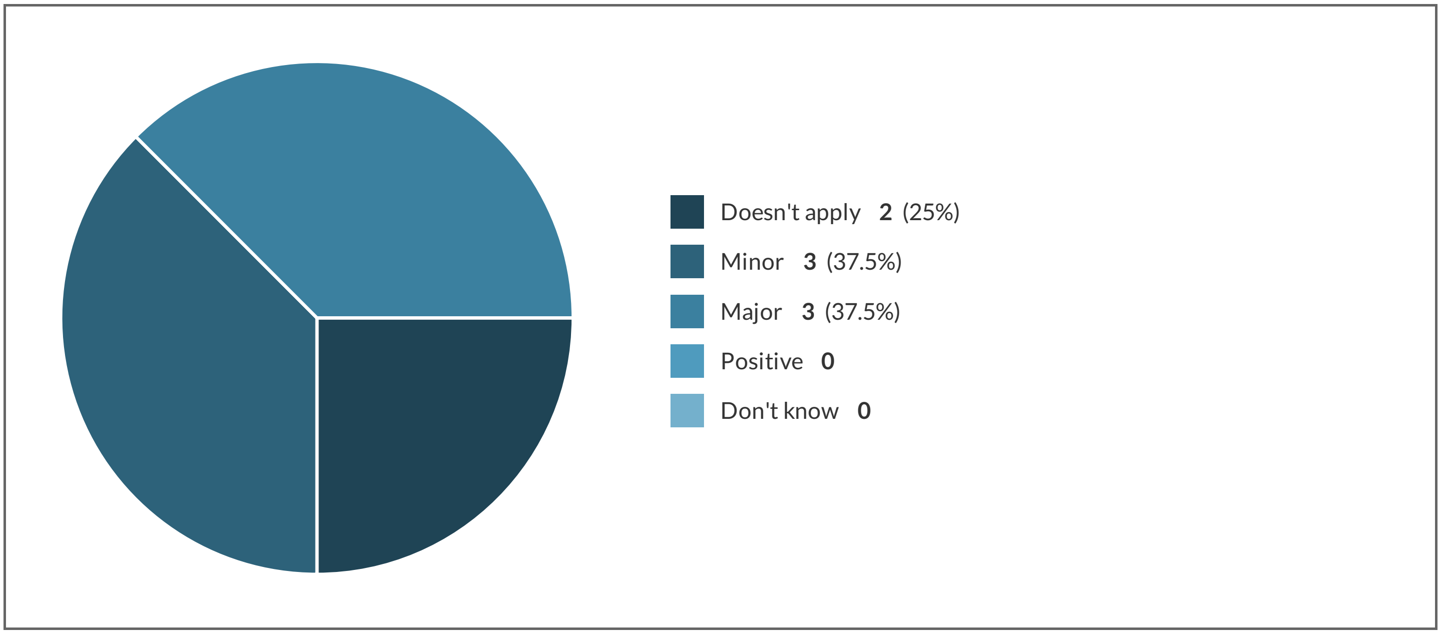


5.1.b Increased help desk/user support time - Frequency Cost is Experienced

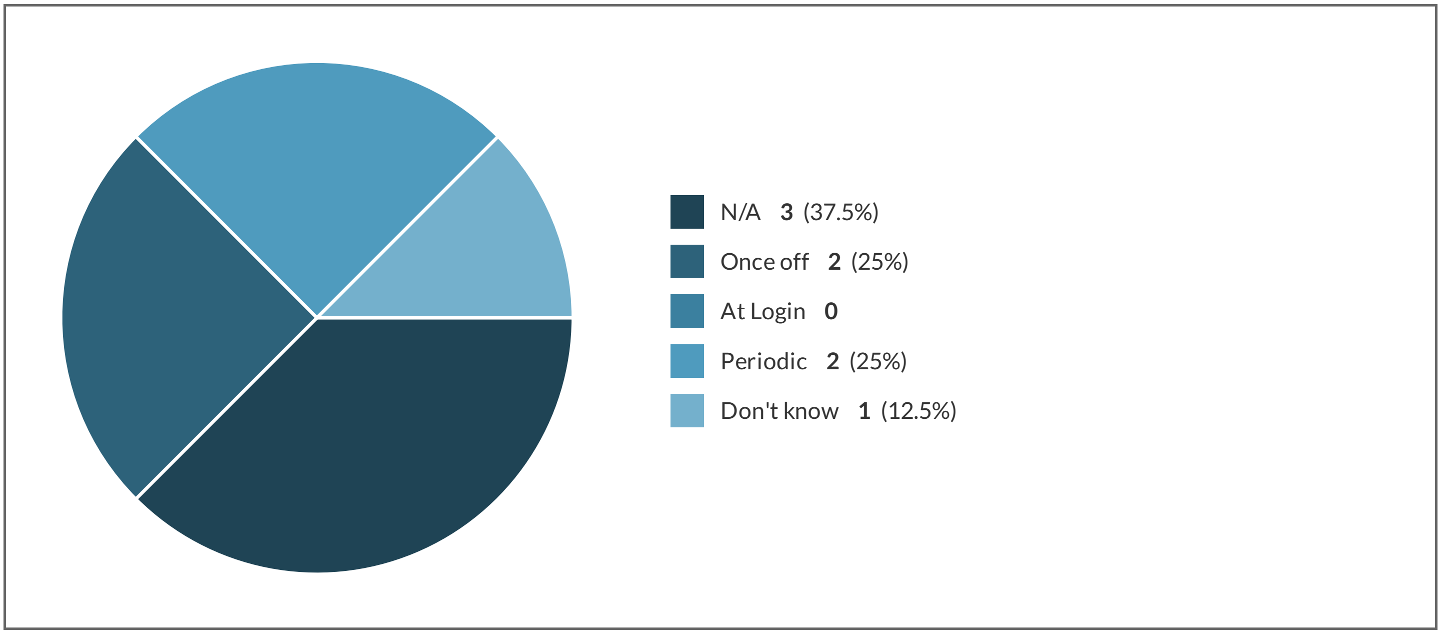


5.2 User education required

5.2.a User education required - Severity of Cost

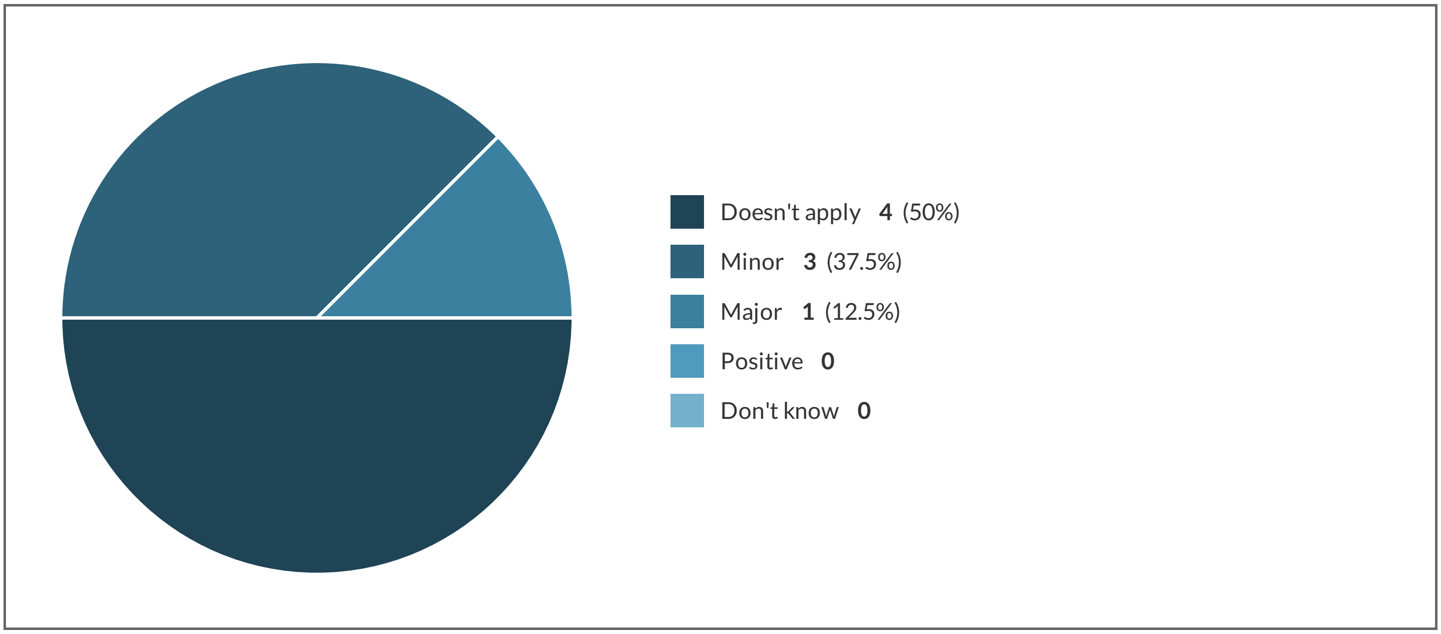


5.2.b User education required - Frequency Cost is Experienced

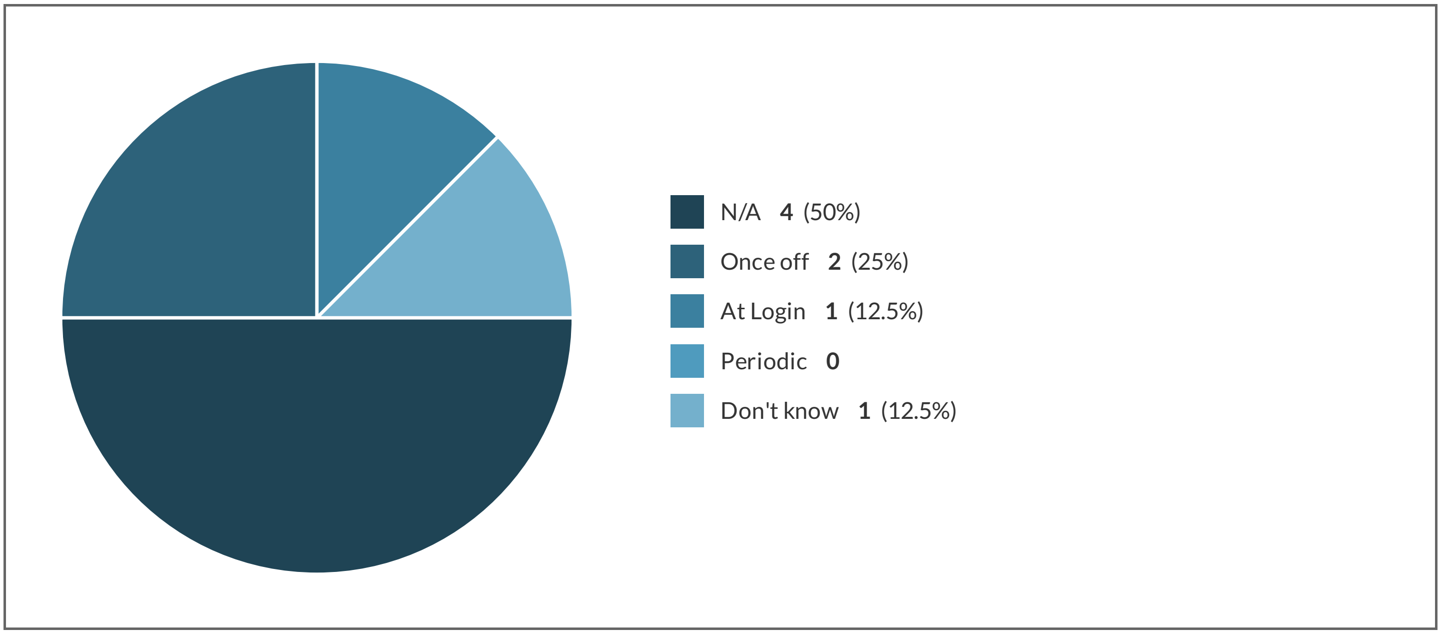


5.3 Organization needs extra resources

5.3.a Organization needs extra resources - Severity of Cost

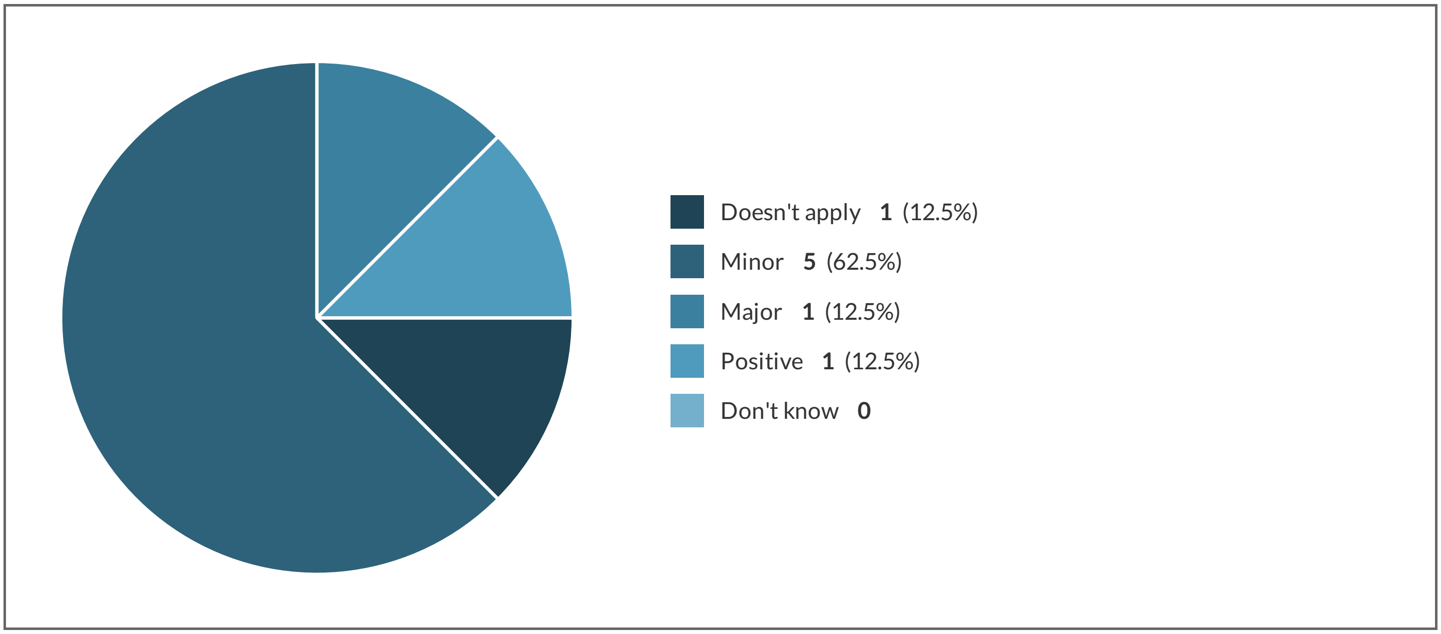


5.3.b Organization needs extra resources - Frequency Cost is Experienced

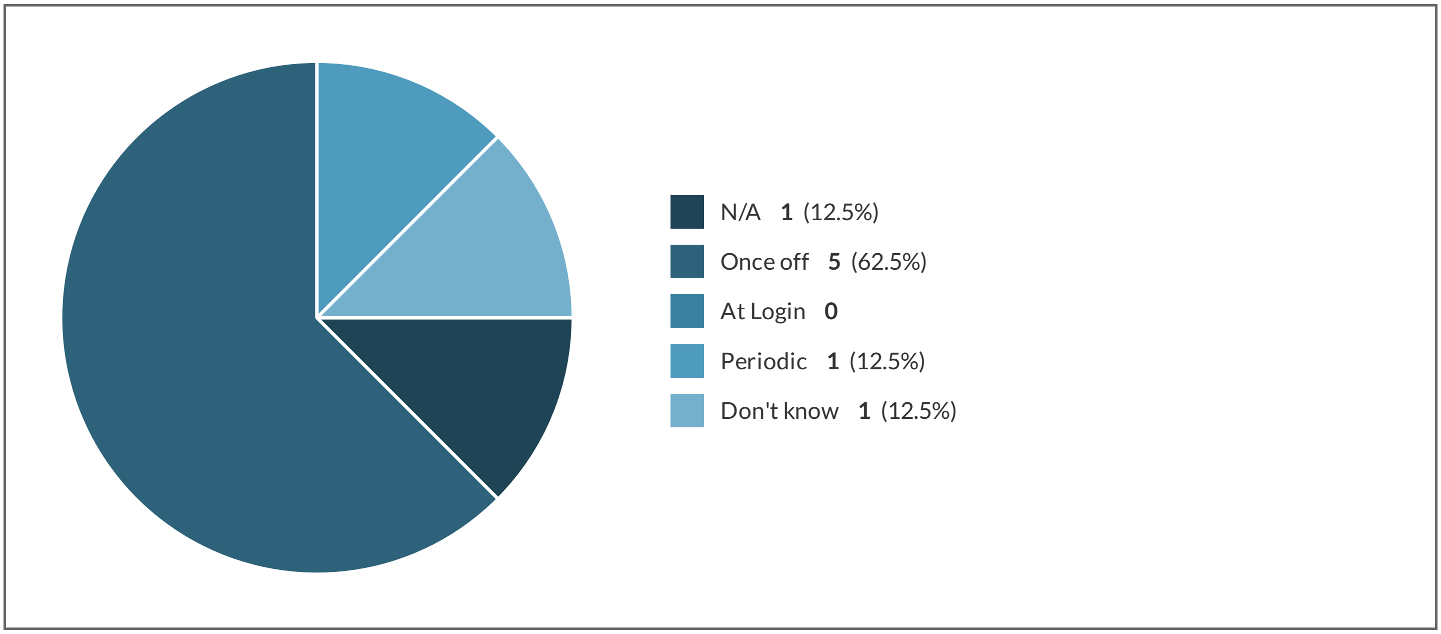


5.4 Takes organization time to implement

5.4.a Takes organization time to implement - Severity of Cost

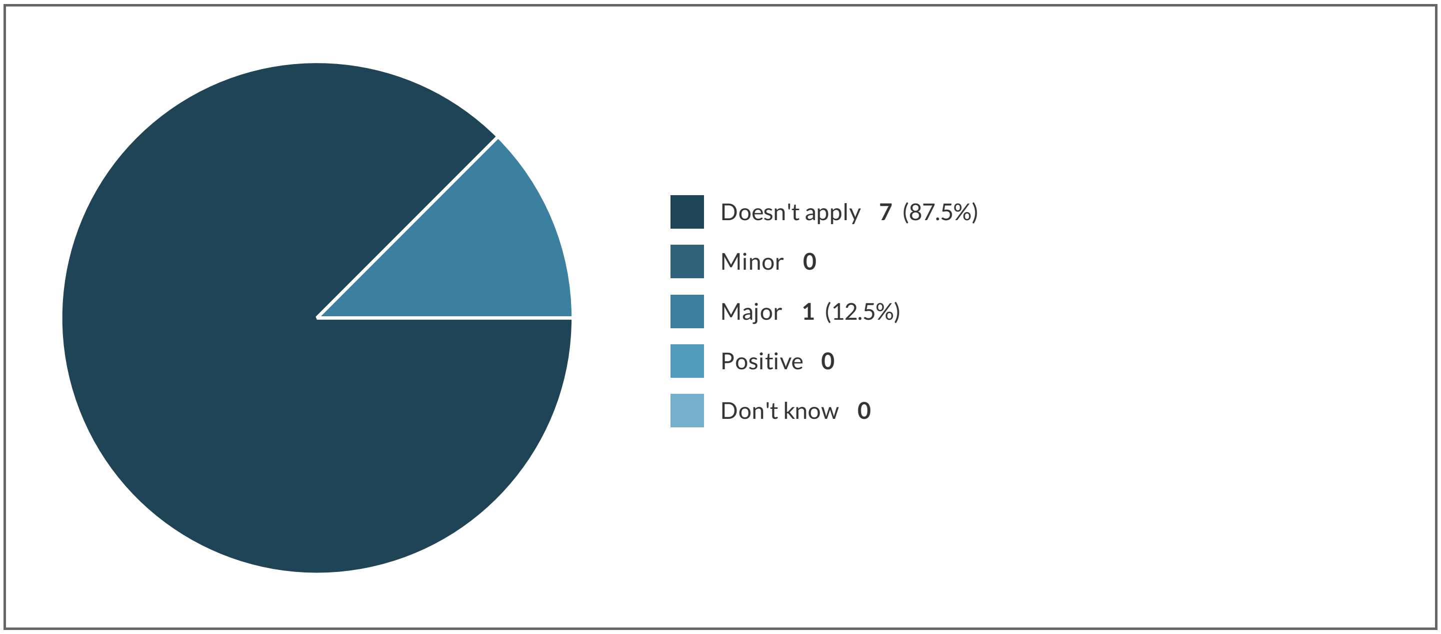


5.4.b Takes organization time to implement - Frequency Cost is Experienced

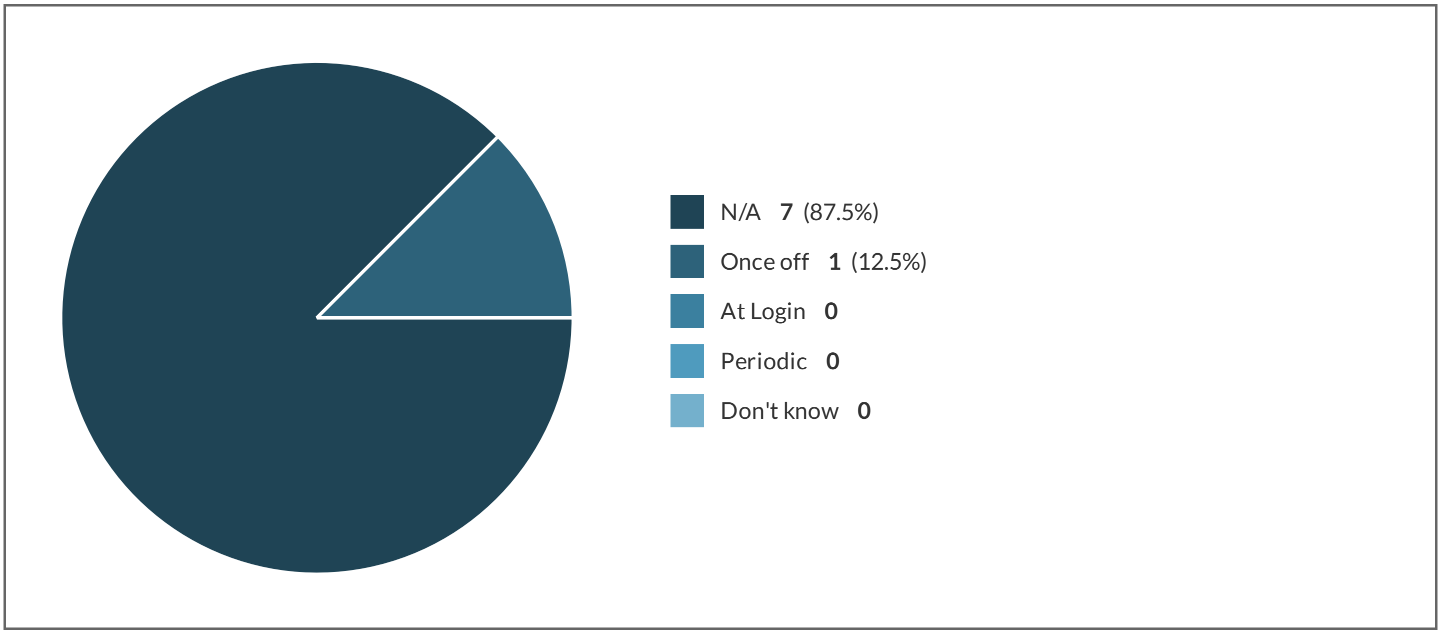


5.5 Increases the organization's computing power needed

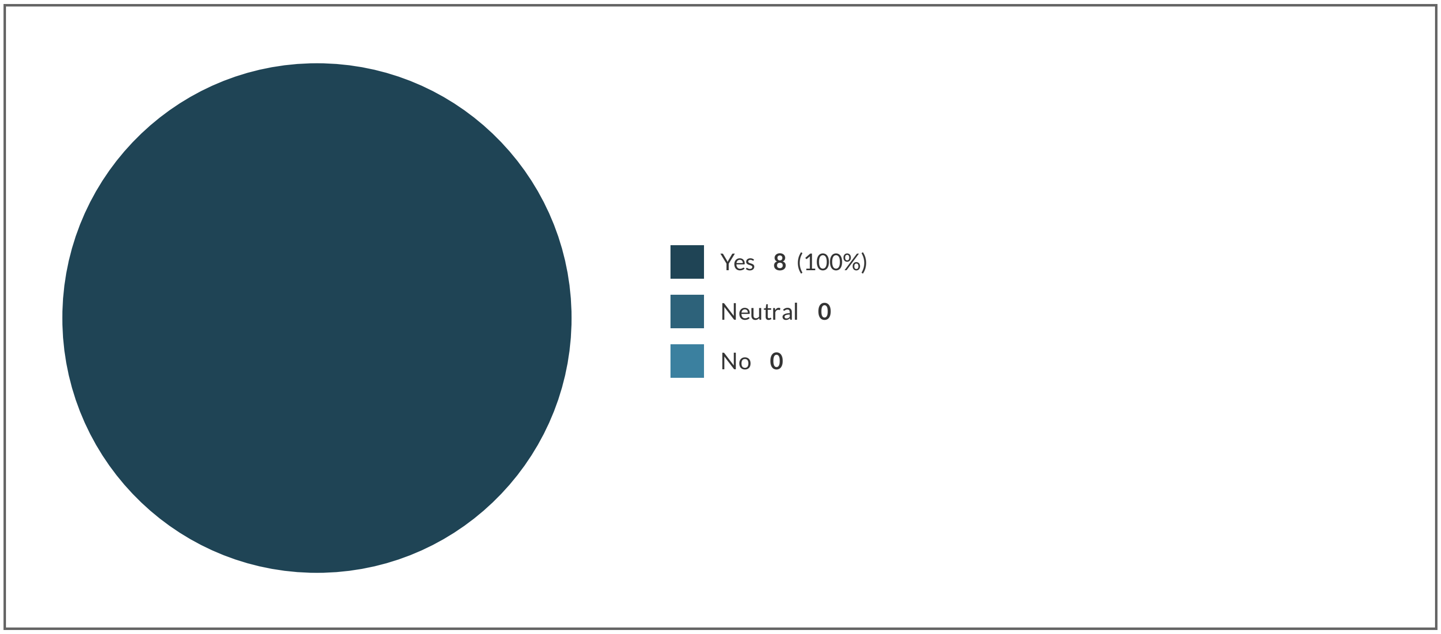
5.5.a Increases the organization's computing power needed - Severity of Cost



5.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



5.a Do you approve of this advice?



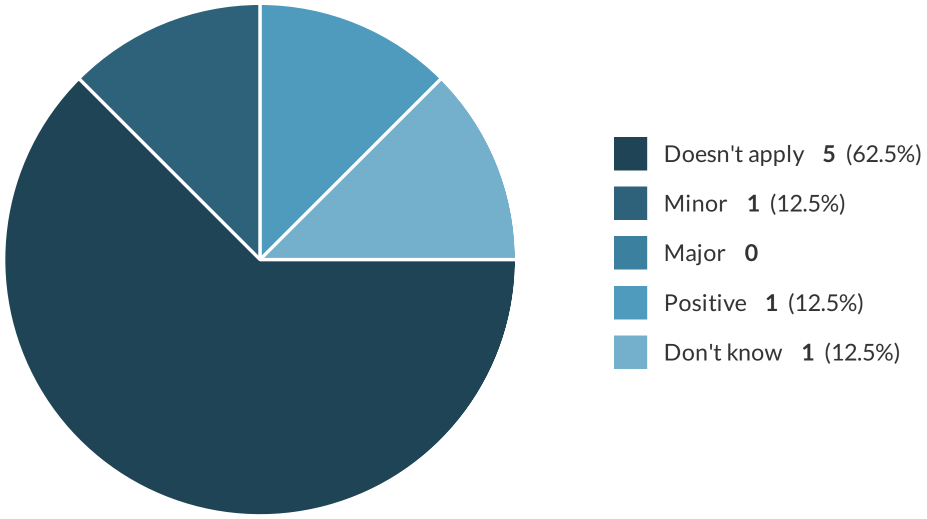
5.b Comments

Showing all 5 responses	
this is done manually at times so it's more time consuming	634211-634202-66098698
This is one of those things where users need continuous advice and support	634211-634202-66532254
The amount of devices I've found on sites that have still using the default factory passwords is shocking	634211-634202-66754804
These default passwords should also be random too, not the same. As an attacker I shouldn't be able to guess a series of emails with a known default password. Minor increase just because the people who tend to leave their passwords as default will now have to remember something else.	634211-634202-66754952
Absolutely	634211-634202-66871889

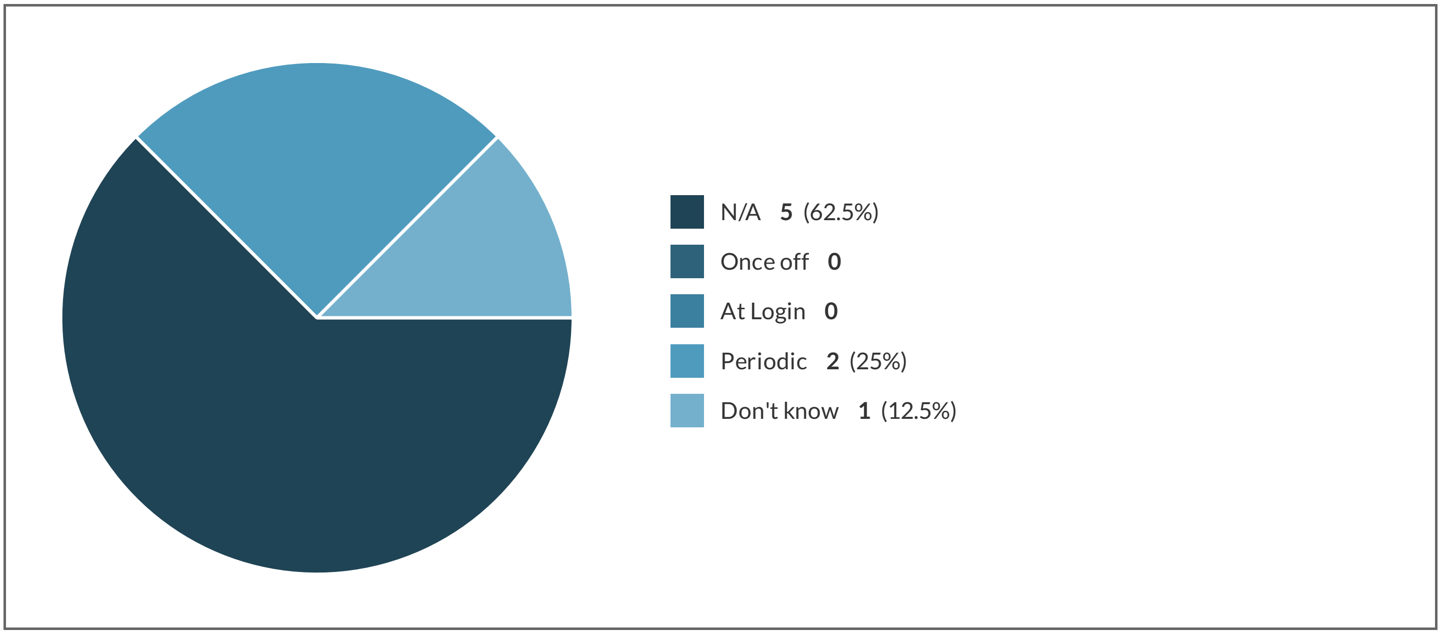
6 Technical Defenses or Controls should be implemented

6.1 Increased help desk/user support time

6.1.a Increased help desk/user support time - Severity of Cost

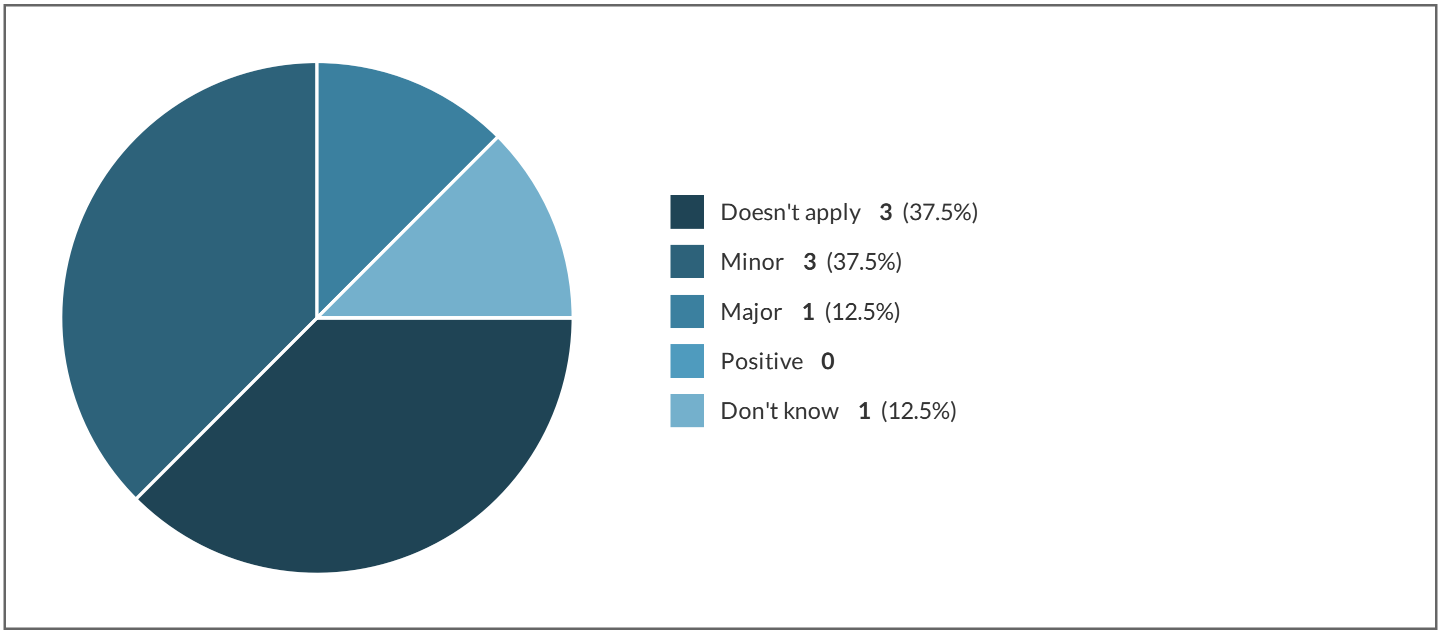


6.1.b Increased help desk/user support time - Frequency Cost is Experienced

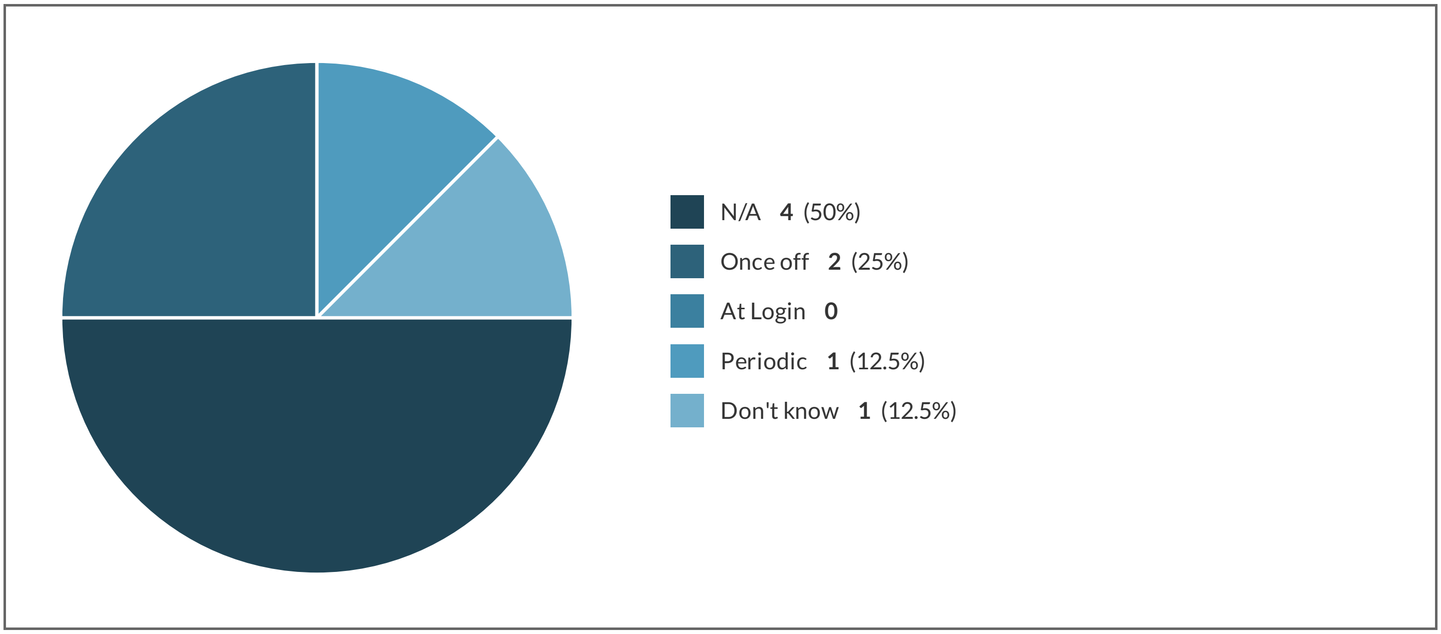


6.2 User education required

6.2.a User education required - Severity of Cost

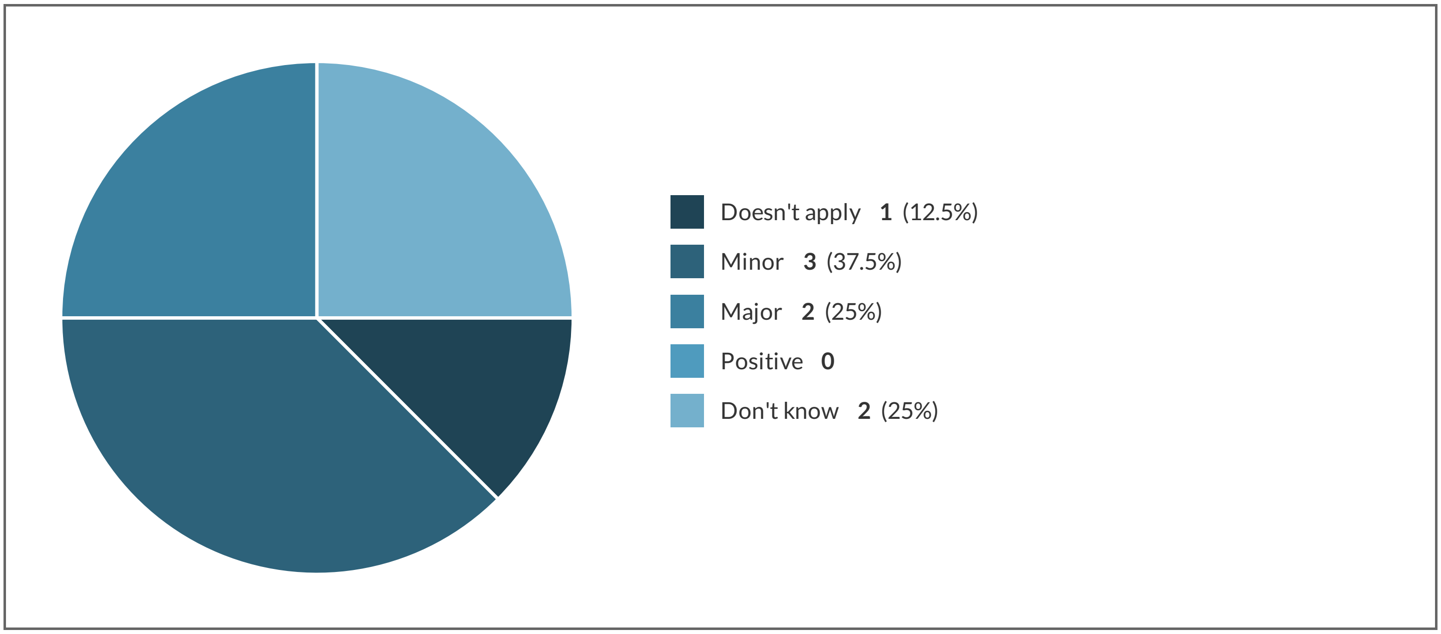


6.2.b User education required - Frequency Cost is Experienced

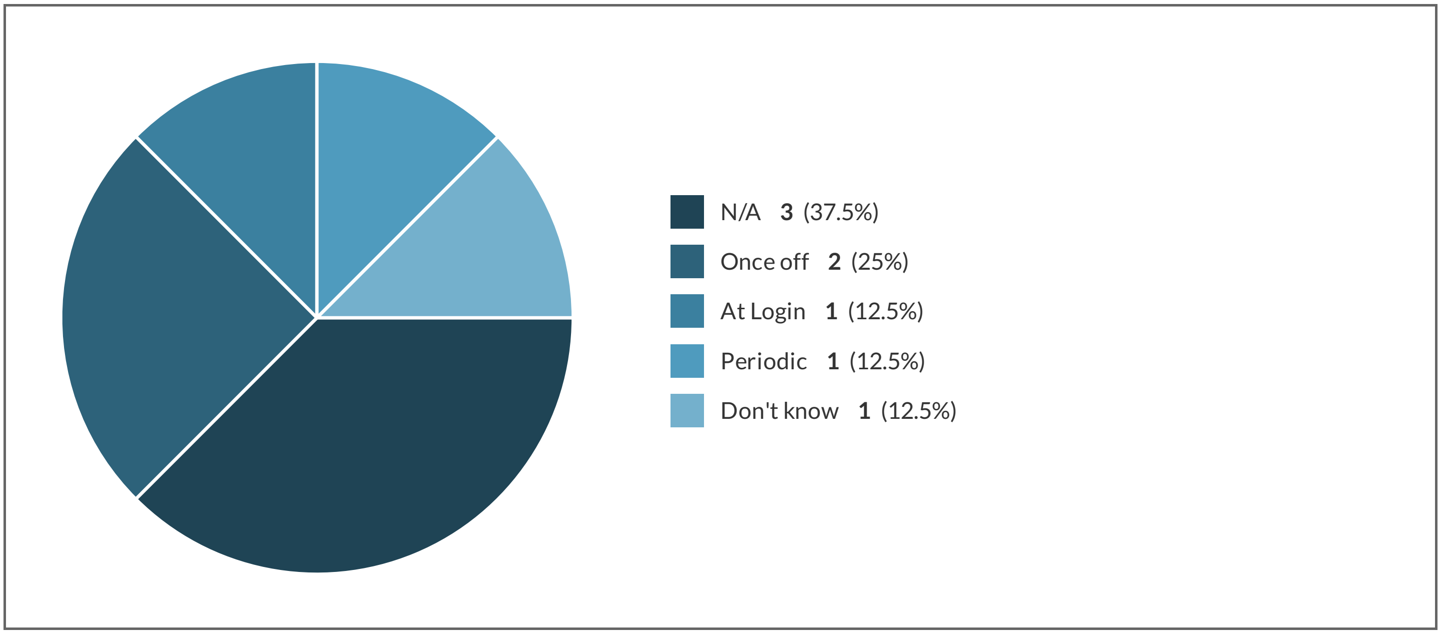


6.3 Organization needs extra resources

6.3.a Organization needs extra resources - Severity of Cost

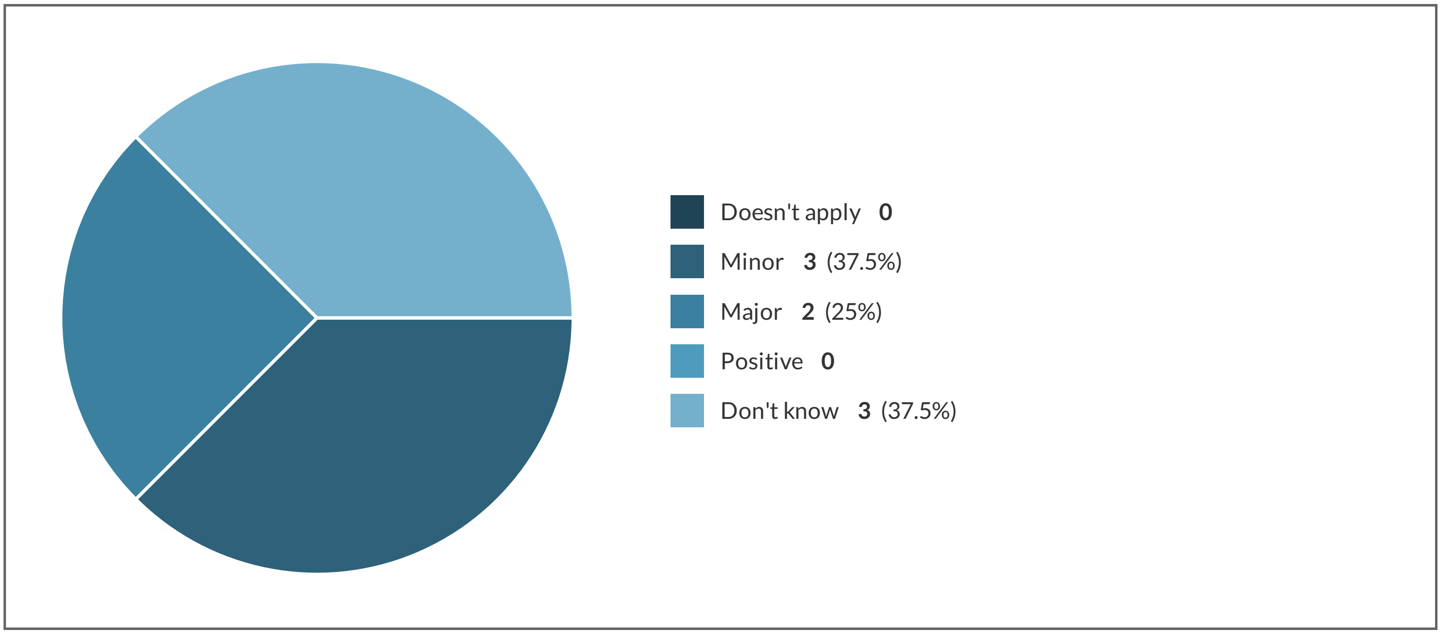


6.3.b Organization needs extra resources - Frequency Cost is Experienced

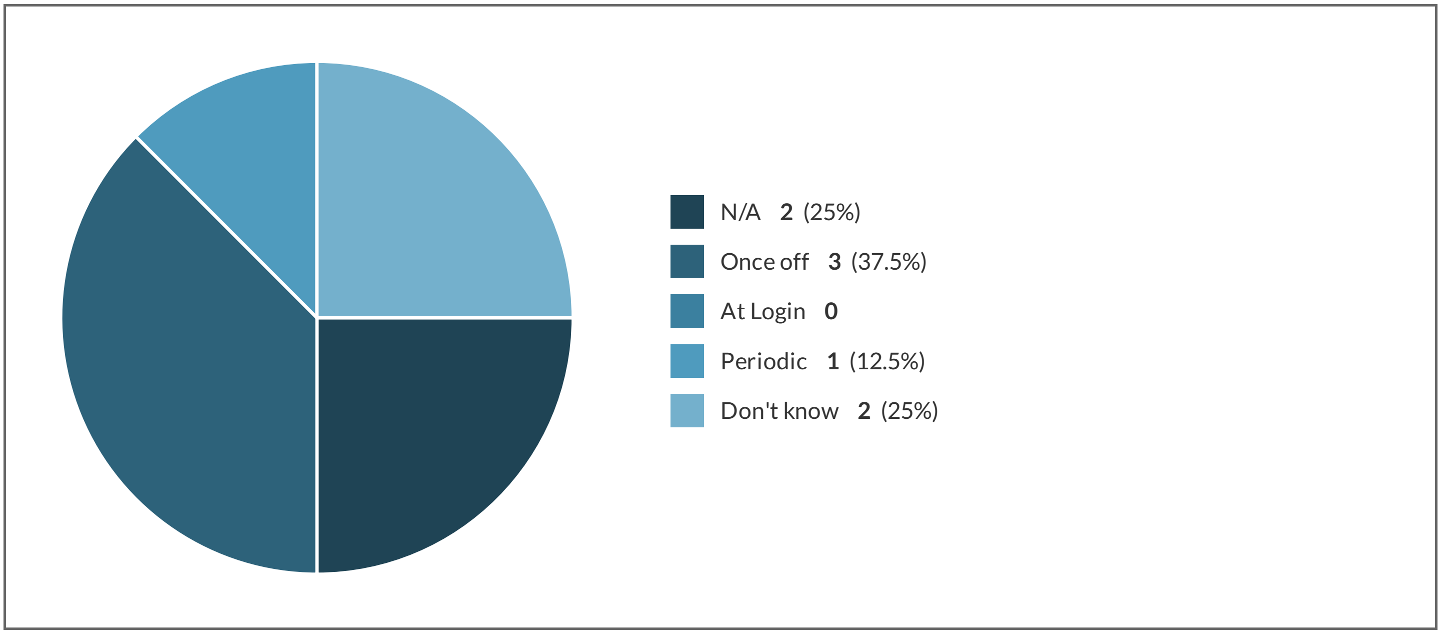


6.4 Takes organization time to implement

6.4.a Takes organization time to implement - Severity of Cost

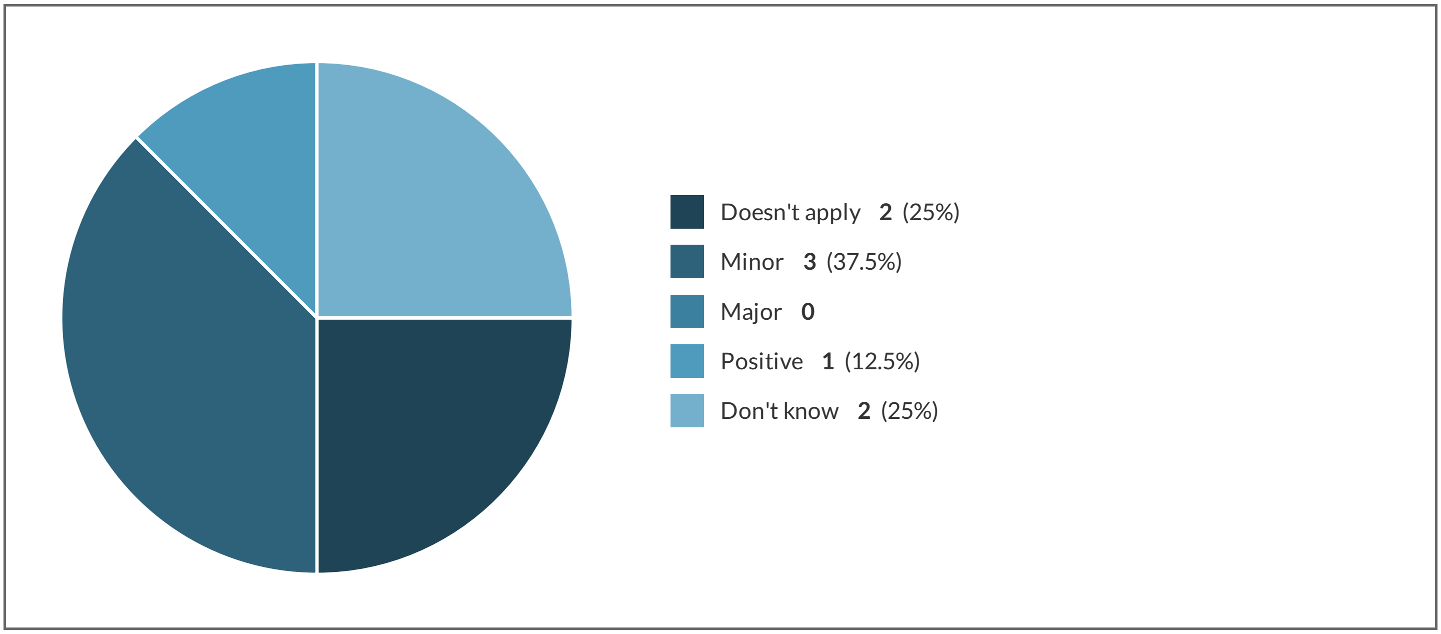


6.4.b Takes organization time to implement - Frequency Cost is Experienced

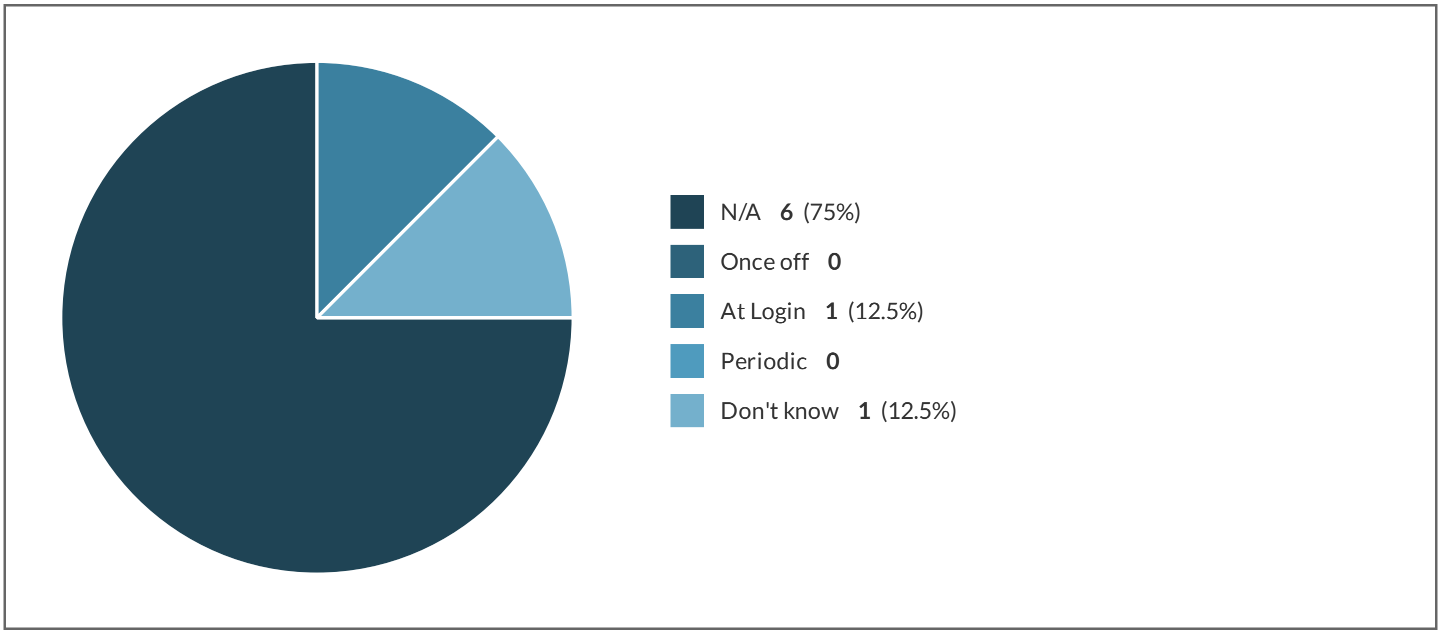


6.5 Increases the organization's computing power needed

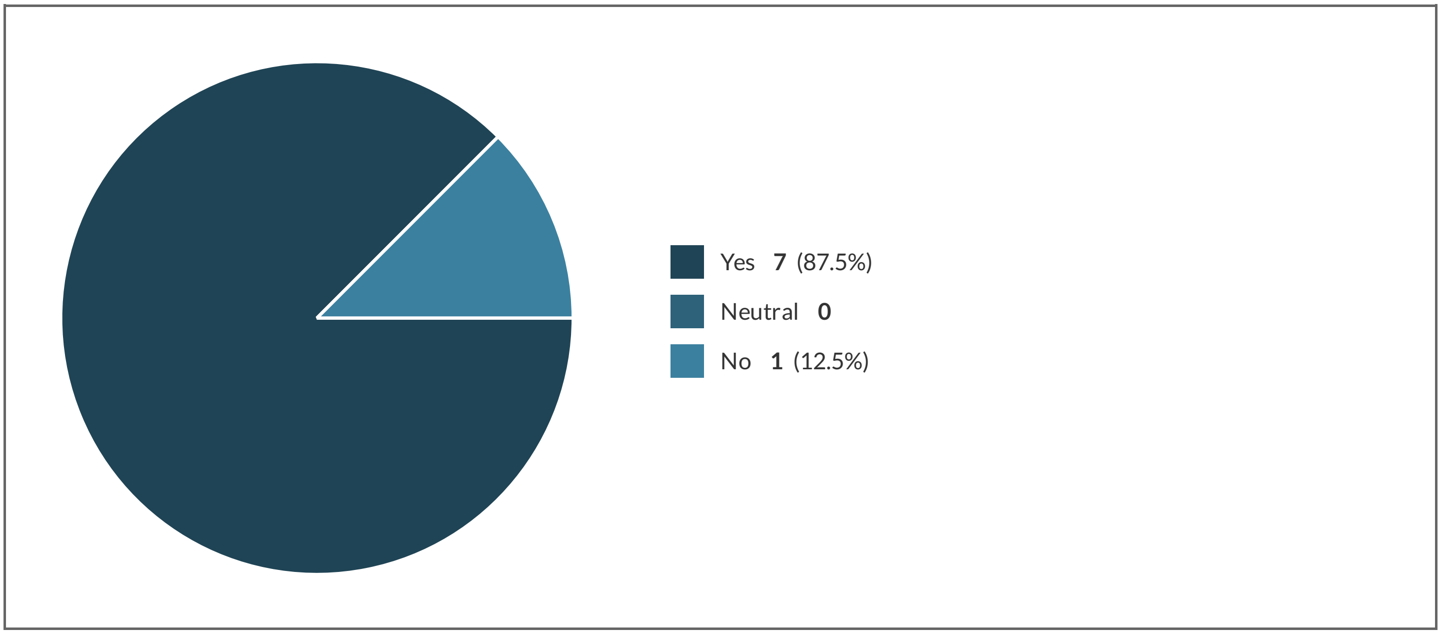
6.5.a Increases the organization's computing power needed - Severity of Cost



6.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



6.a Do you approve of this advice?



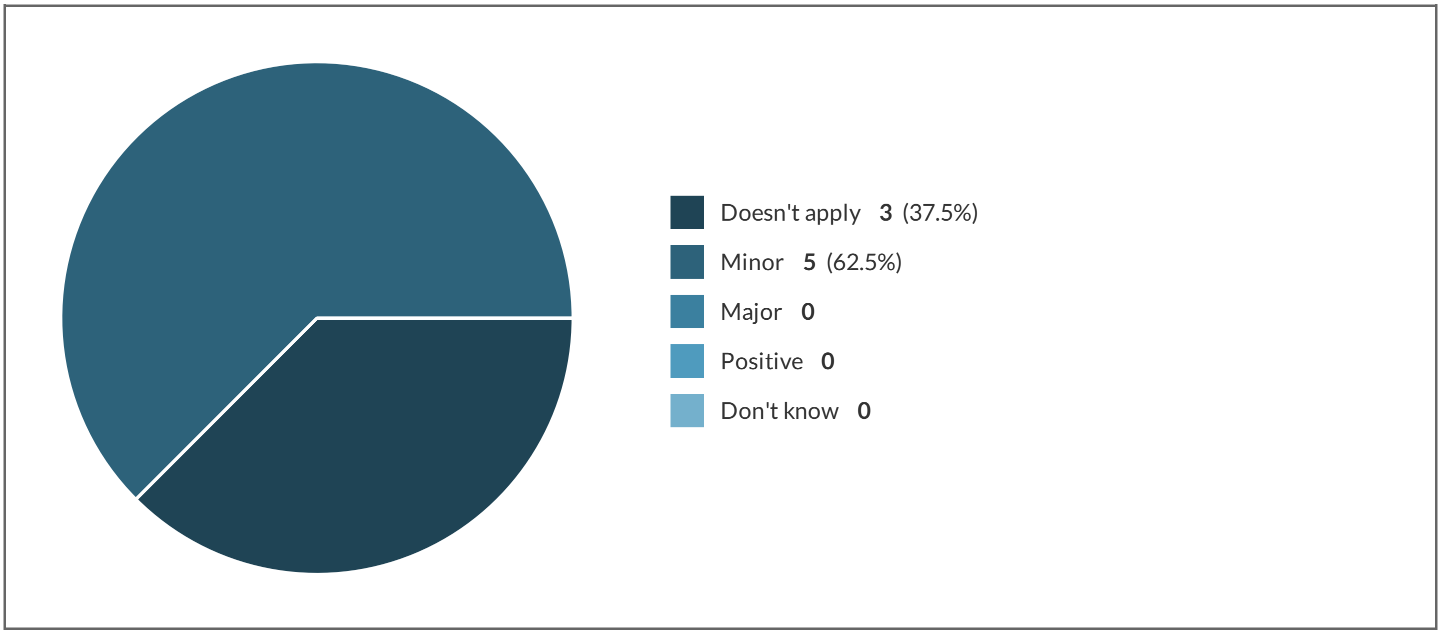
6.b Comments

Showing all 4 responses	
Not specific or meaningful enough to be useful advice	634211-634202-66532254
The amount of company's that barely have edge firewalls protecting there company's in shocking and its relatively simple to implement	634211-634202-66754804
I would go as far as saying MFA should be mandatory any company resources should have to be accessed over a vpn and the access policy on that VPN should have you running some sort of company approved anti-virus (sophos or fireeye for example).	634211-634202-66754952
The question is too open ended to assess probably costs.	634211-634202-66871889

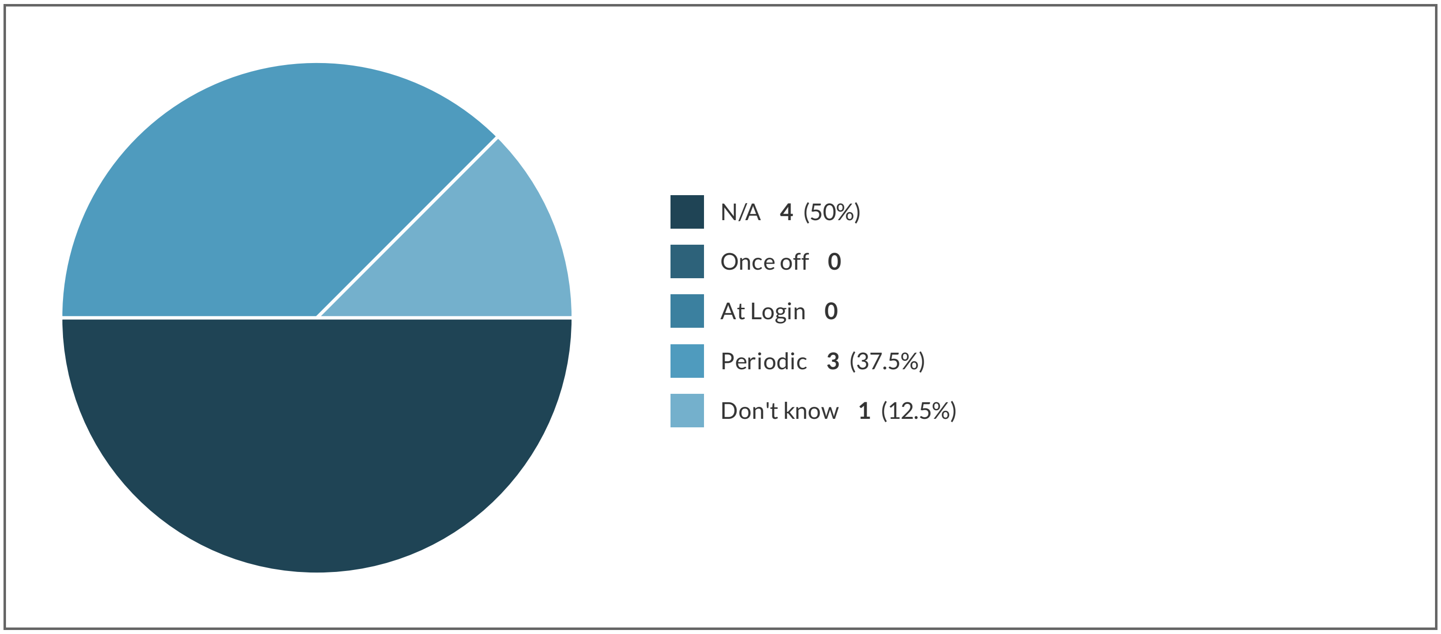
7 Composition rules should be enforced for passwords (e.g. must have letters, numbers and a special character)

7.1 Increased help desk/user support time

7.1.a Increased help desk/user support time - Severity of Cost

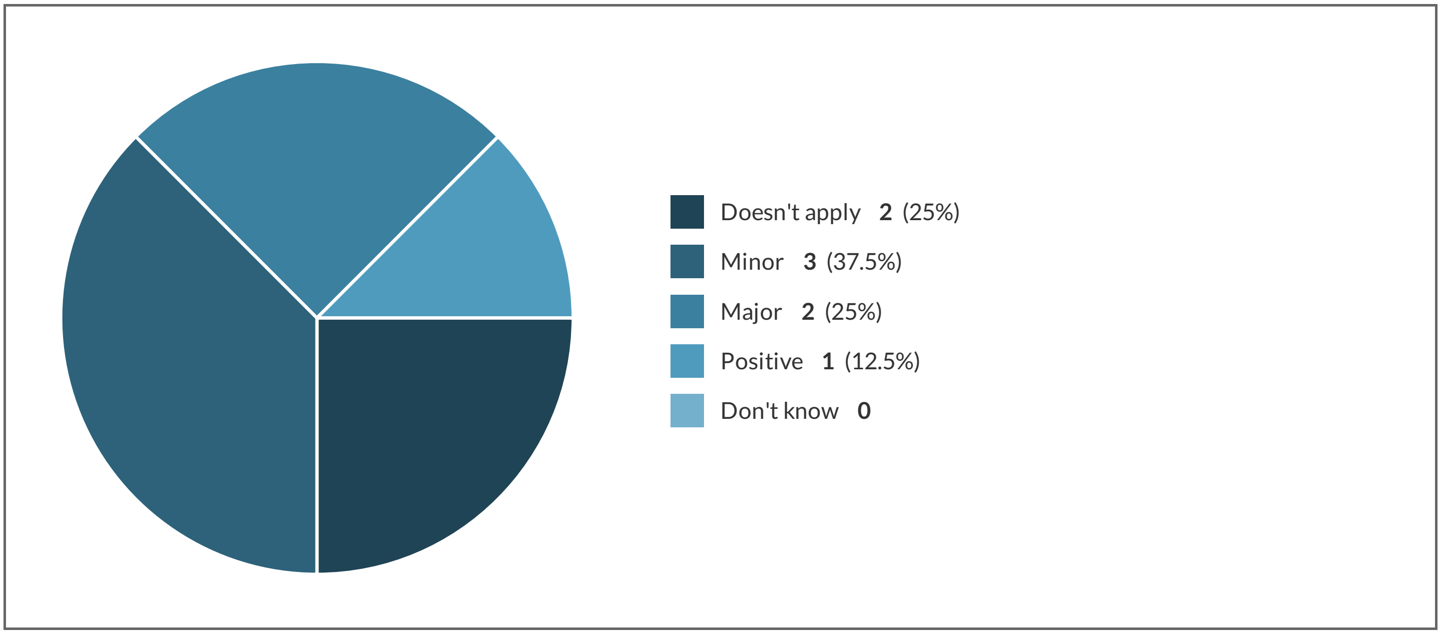


7.1.b Increased help desk/user support time - Frequency Cost is Experienced

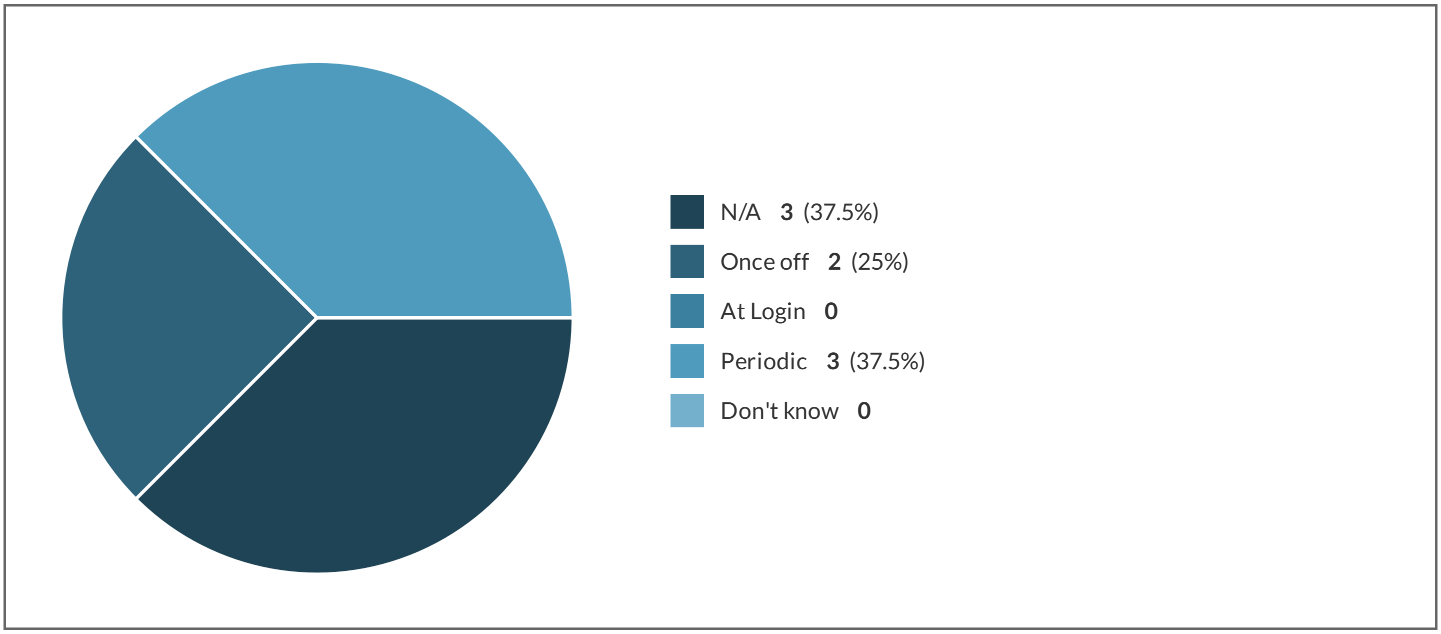


7.2 User education required

7.2.a User education required - Severity of Cost

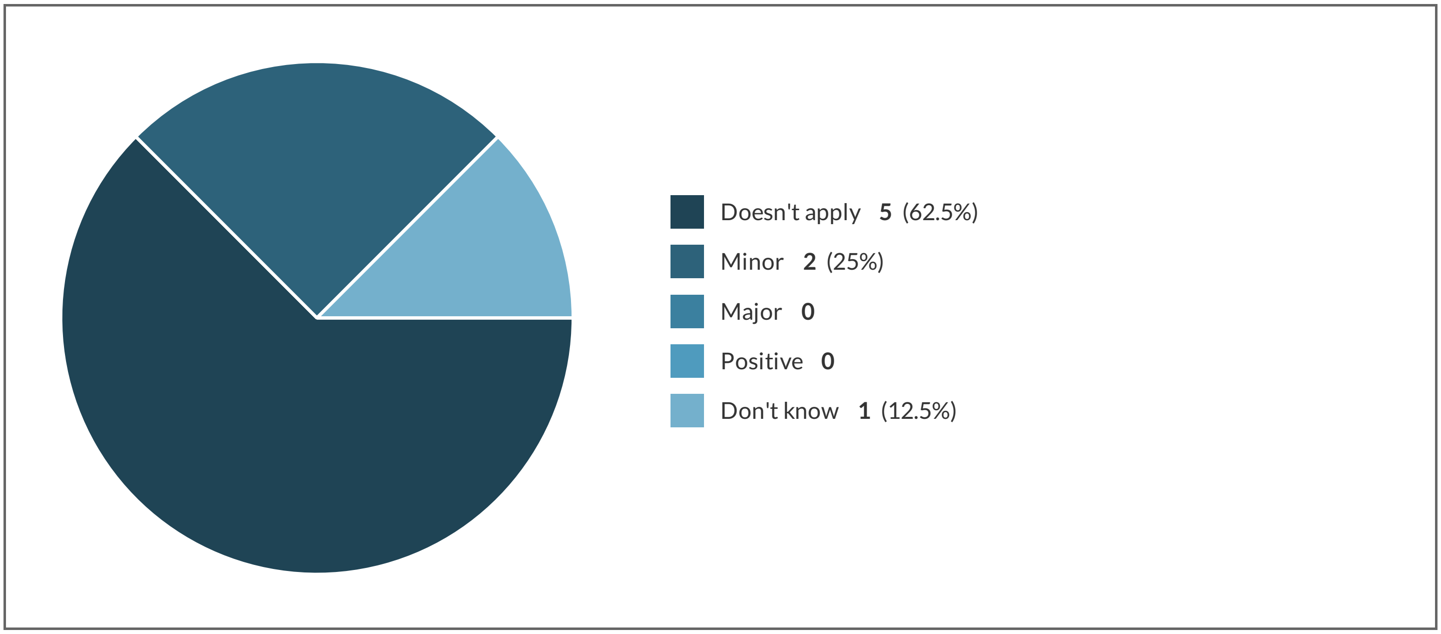


7.2.b User education required - Frequency Cost is Experienced

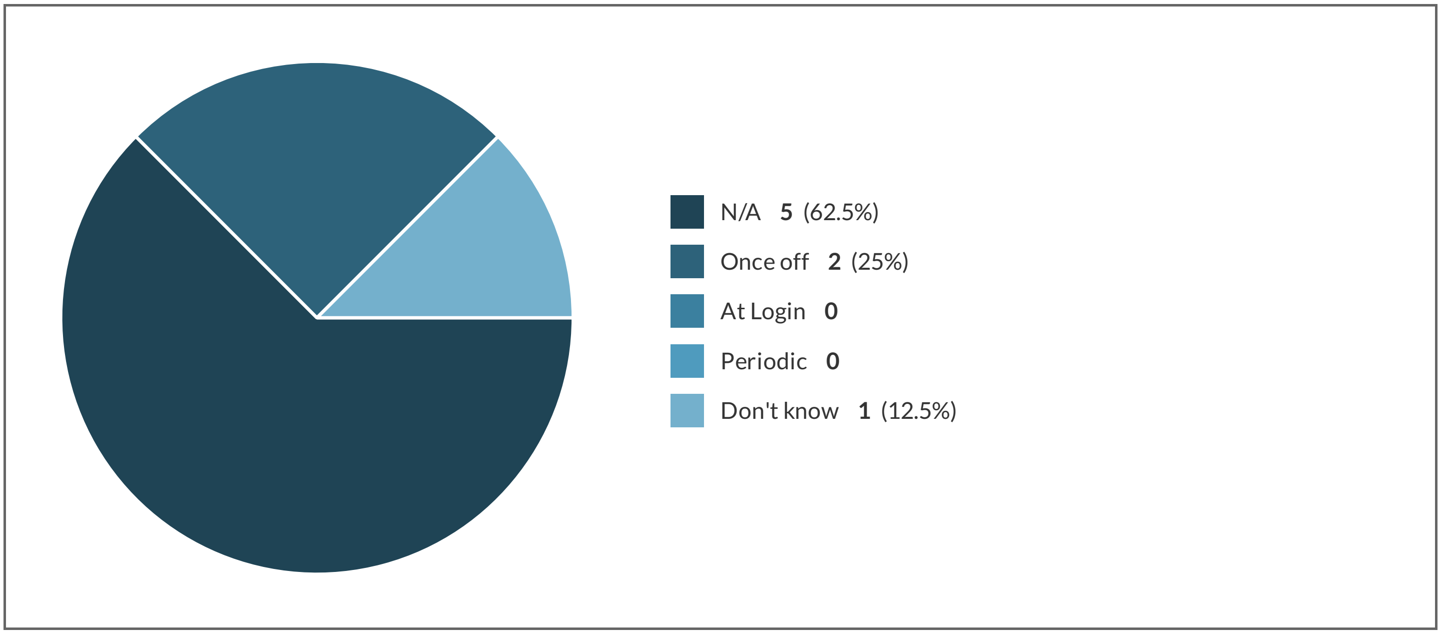


7.3 Organization needs extra resources

7.3.a Organization needs extra resources - Severity of Cost

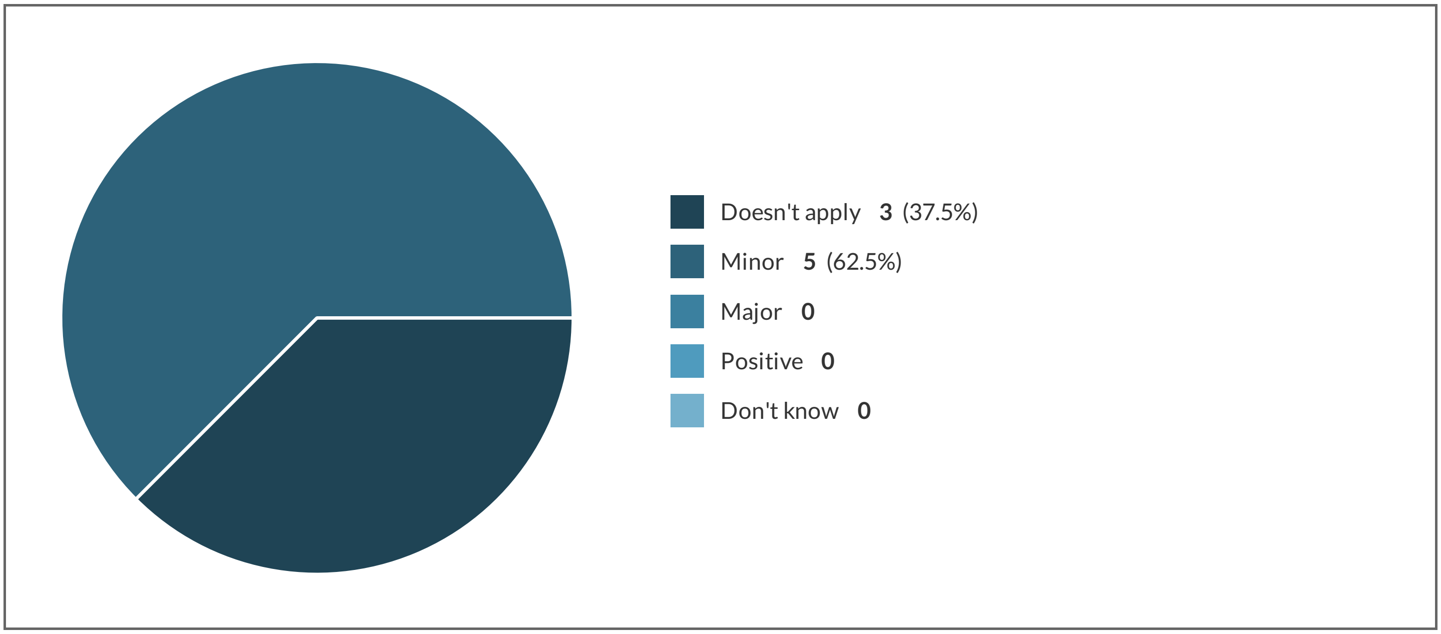


7.3.b Organization needs extra resources - Frequency Cost is Experienced

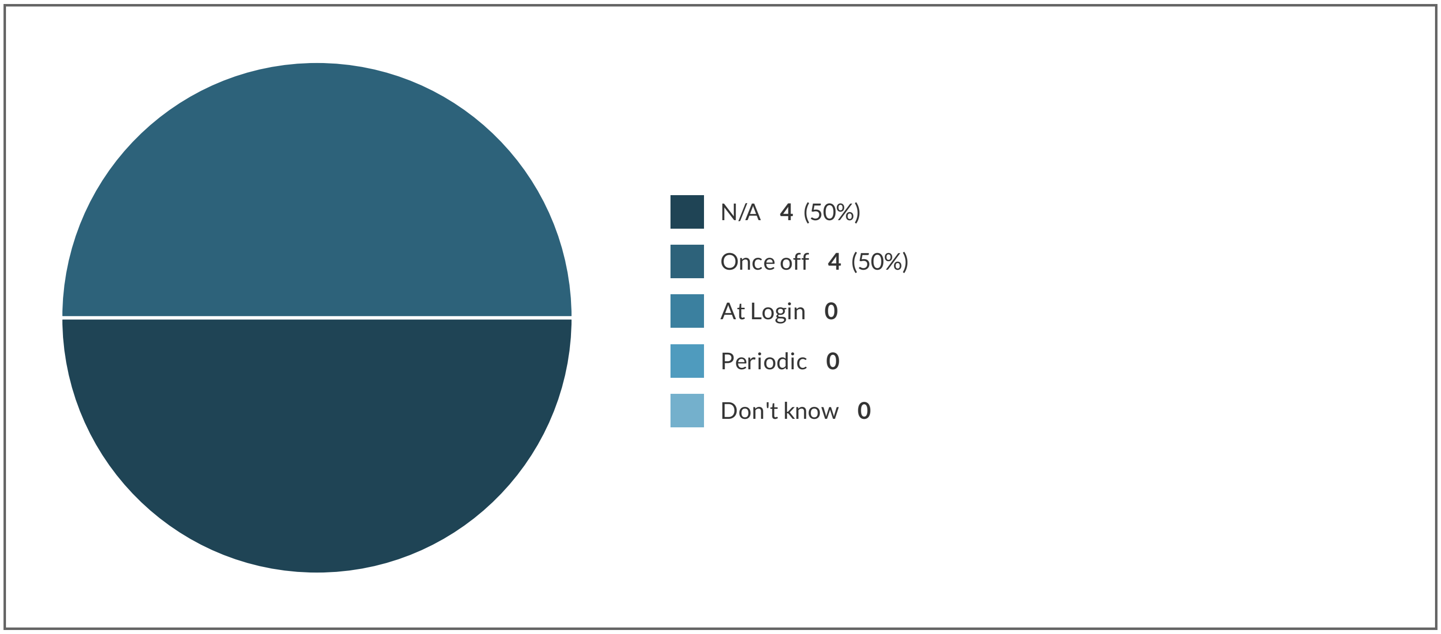


7.4 Takes organization time to implement

7.4.a Takes organization time to implement - Severity of Cost

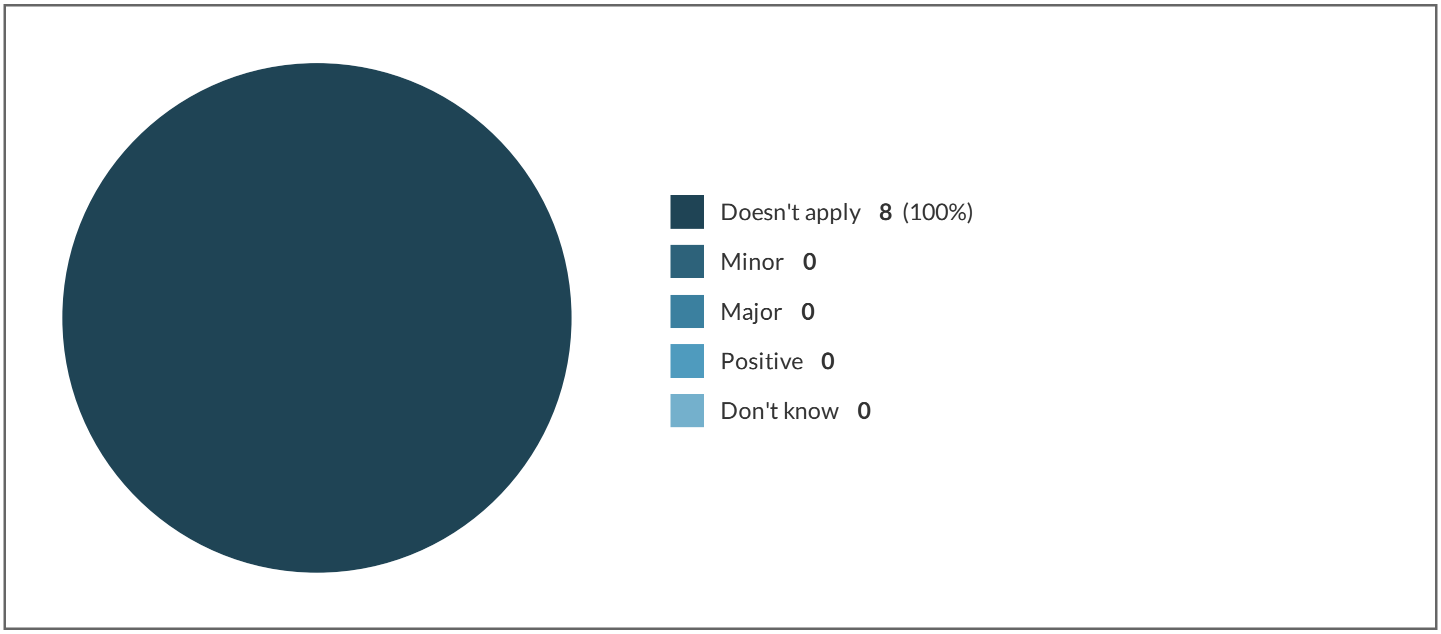


7.4.b Takes organization time to implement - Frequency Cost is Experienced

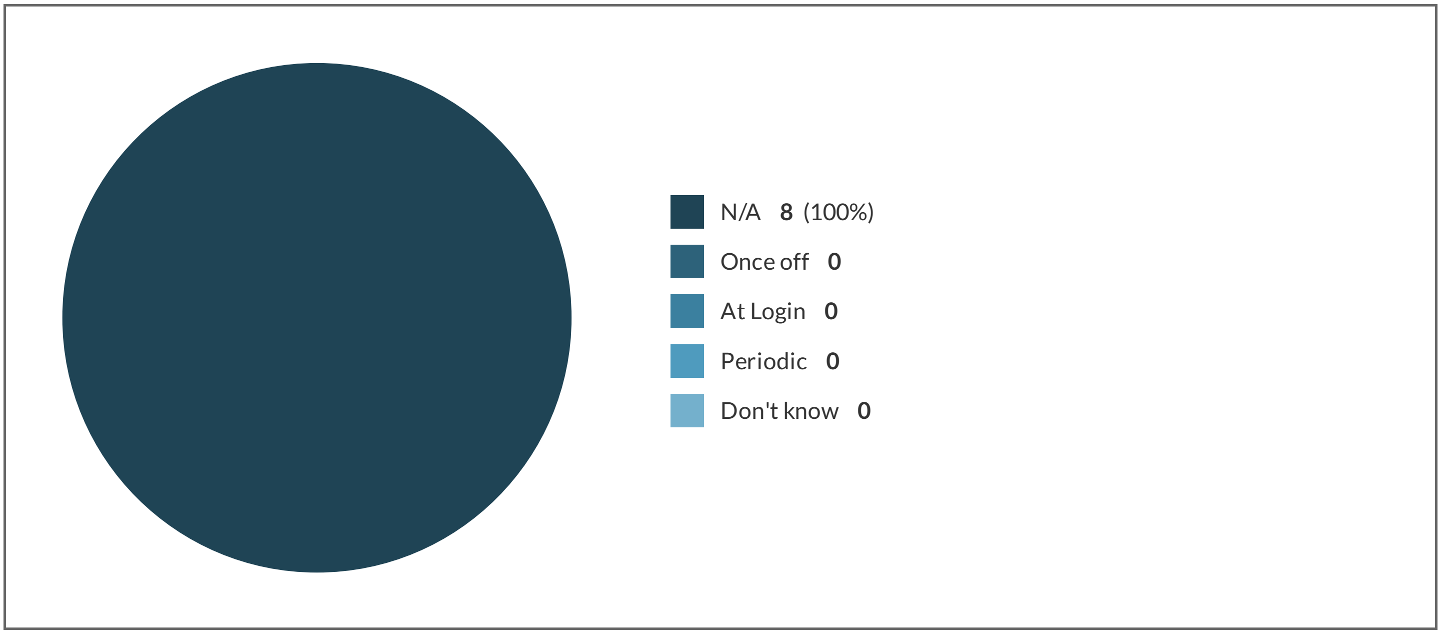


7.5 Increases the organization's computing power needed

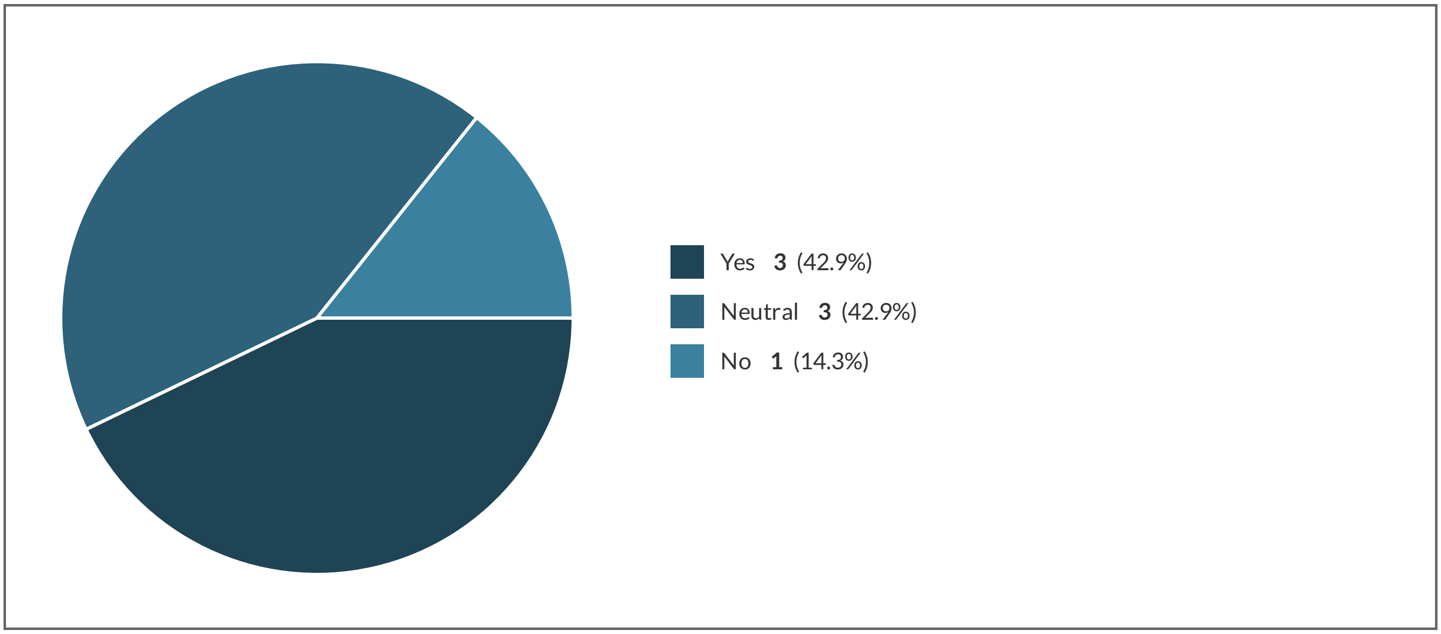
7.5.a Increases the organization's computing power needed - Severity of Cost



7.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



7.a Do you approve of this advice?



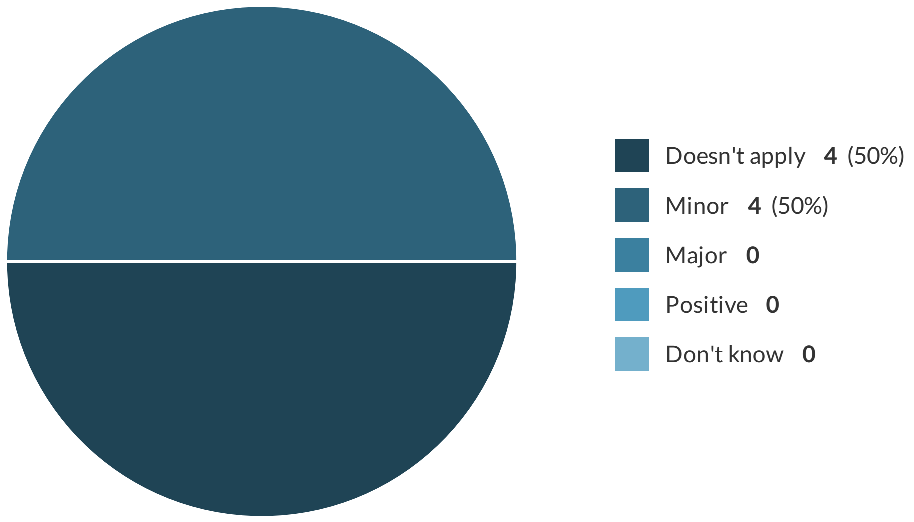
7.b Comments

Showing all 4 responses	
In certain circumstances. Passphrases with sufficient additional complexity to increase entropy are a better idea than passwords are difficult to remember but easy to brute force.	634211-634202-66090277
See above re occasional password changes	634211-634202-66532254
As I've worked in major multi national company's this policy is the norm when it comes to compositiom rules	634211-634202-66754804
So I kind of hate composition rules. If I as an attacker get access to a dump of hashed passwords or try to brute force a login and I know their composition policy (which seeing as most companies use the same 1 upper 1 lower 1 number and 1 symbol policy isn't that hard to imagine) there are actually now less combinations I have to worry about due to the fact that I know these now have to contain a letter/number/special character. We also know that these characters will generally fall into 3 categories 1. post-fix e.g. password1 or password$ 2. Separator e.g. my_password 3. Substitution e.g. p@ssw0rd all of those example passwords would be valid under a composition rule and they are all incredibly common and with common usage patterns to guess, it also helps (helps the attacker that is) that passwords with these extra requirements tend to be shorter due to the characters and numbers making them harder to remember. So really what we have ended up doing with composition rules is we've made passwords easier for computers to guess and harder for users to remember.	634211-634202-66754952

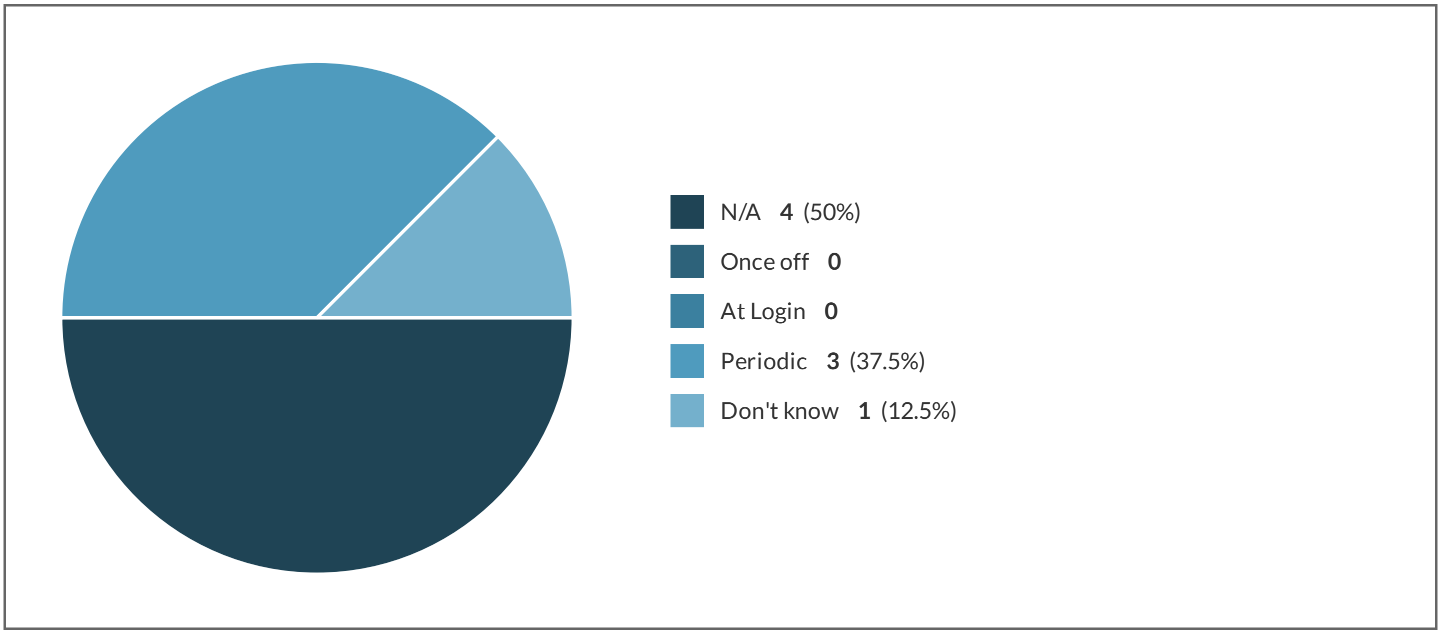
8 Length restrictions for passwords should be enforced (e.g. password must be at least 8 characters)

8.1 Increased help desk/user support time

8.1.a Increased help desk/user support time - Severity of Cost

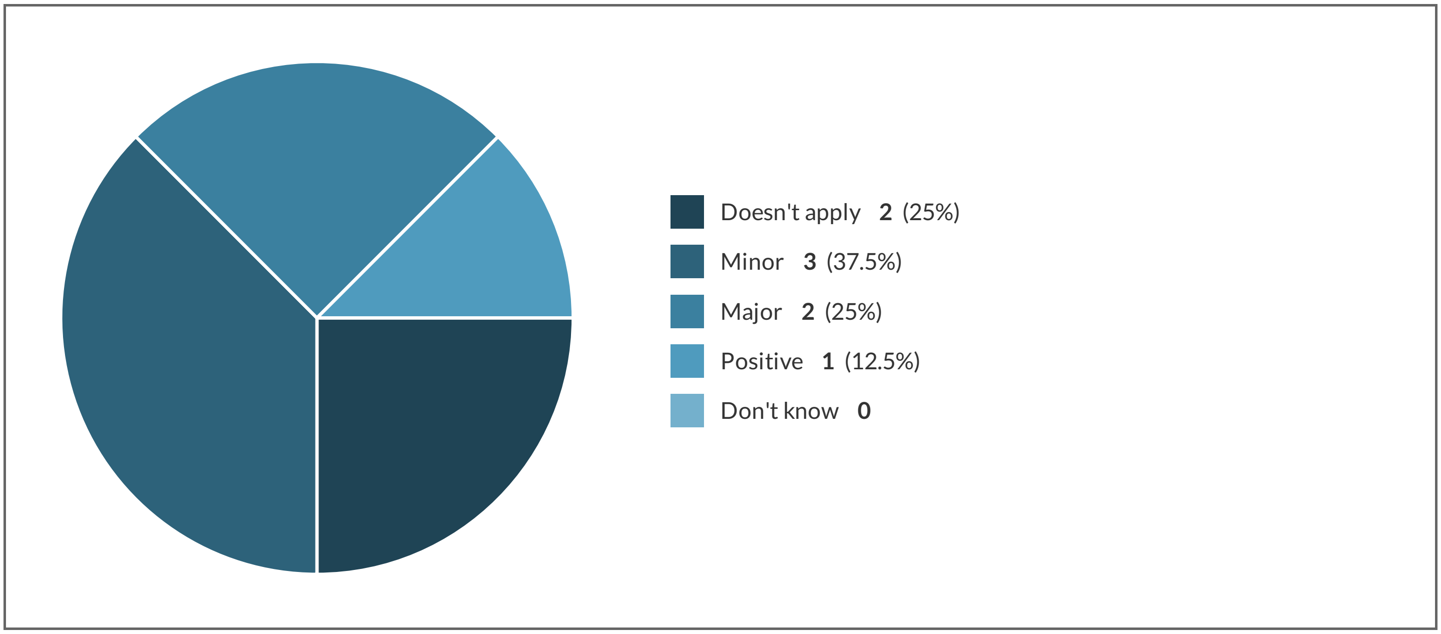


8.1.b Increased help desk/user support time - Frequency Cost is Experienced

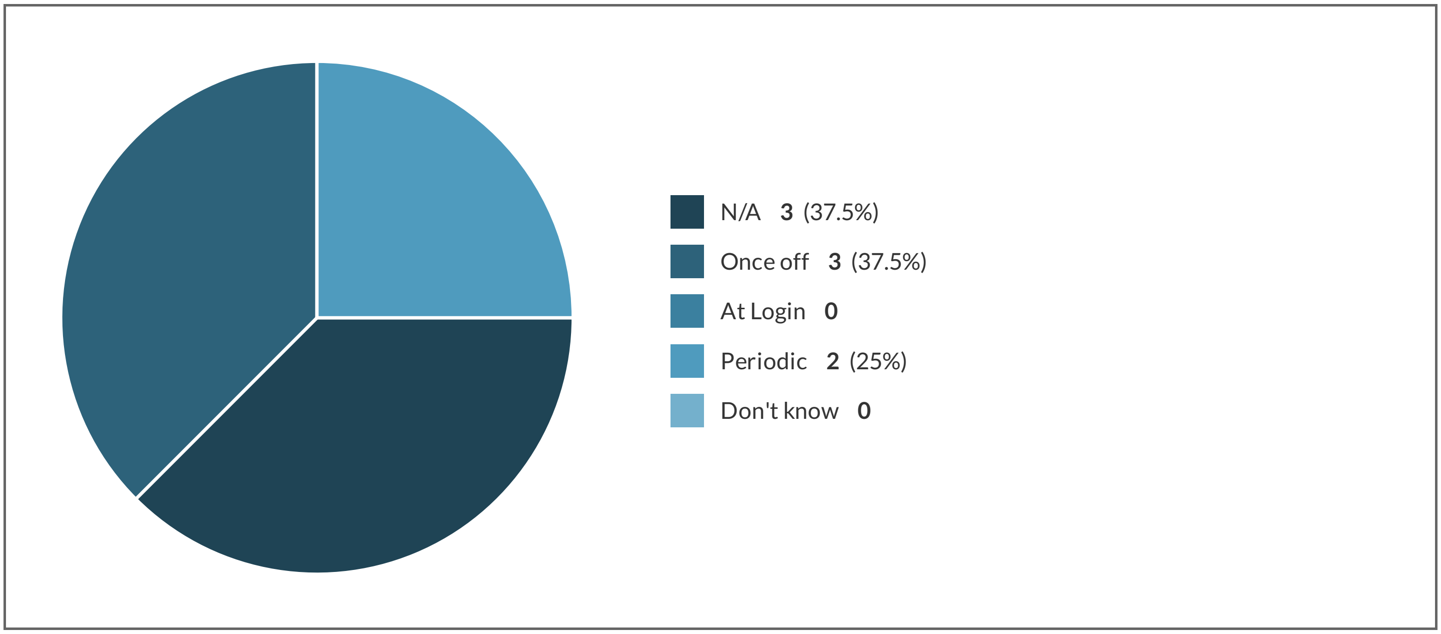


8.2 User education required

8.2.a User education required - Severity of Cost

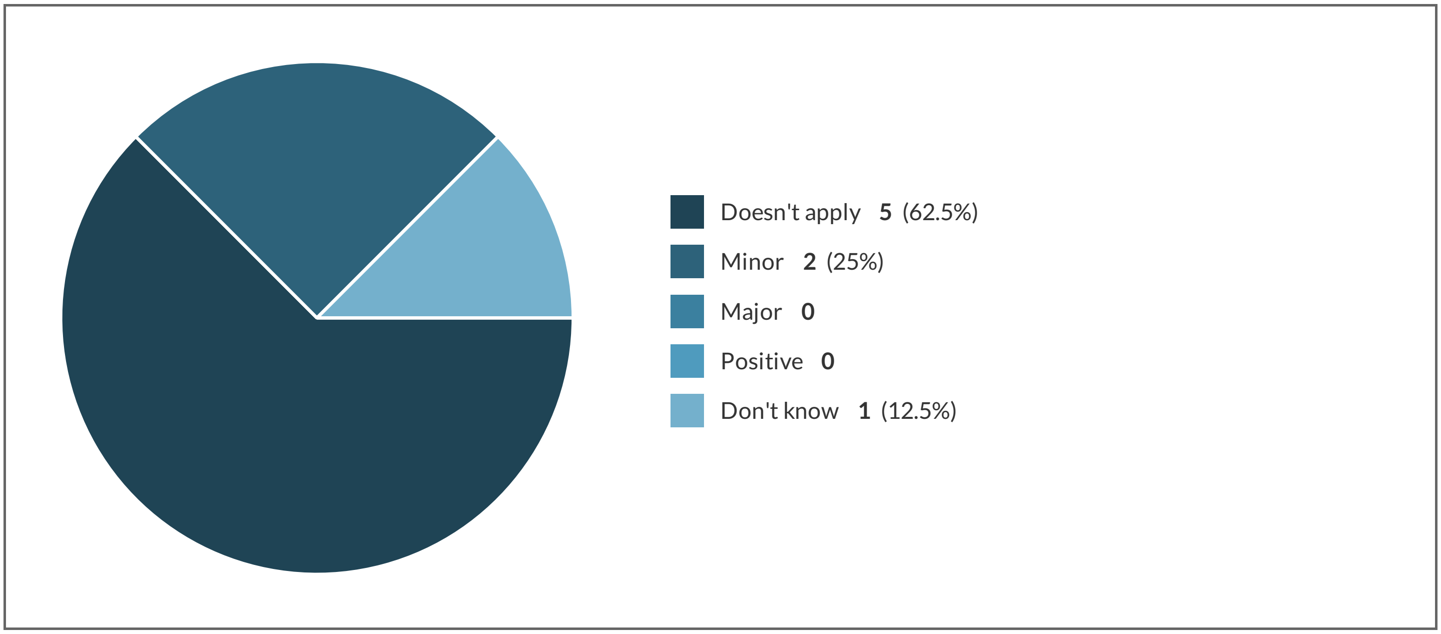


8.2.b User education required - Frequency Cost is Experienced

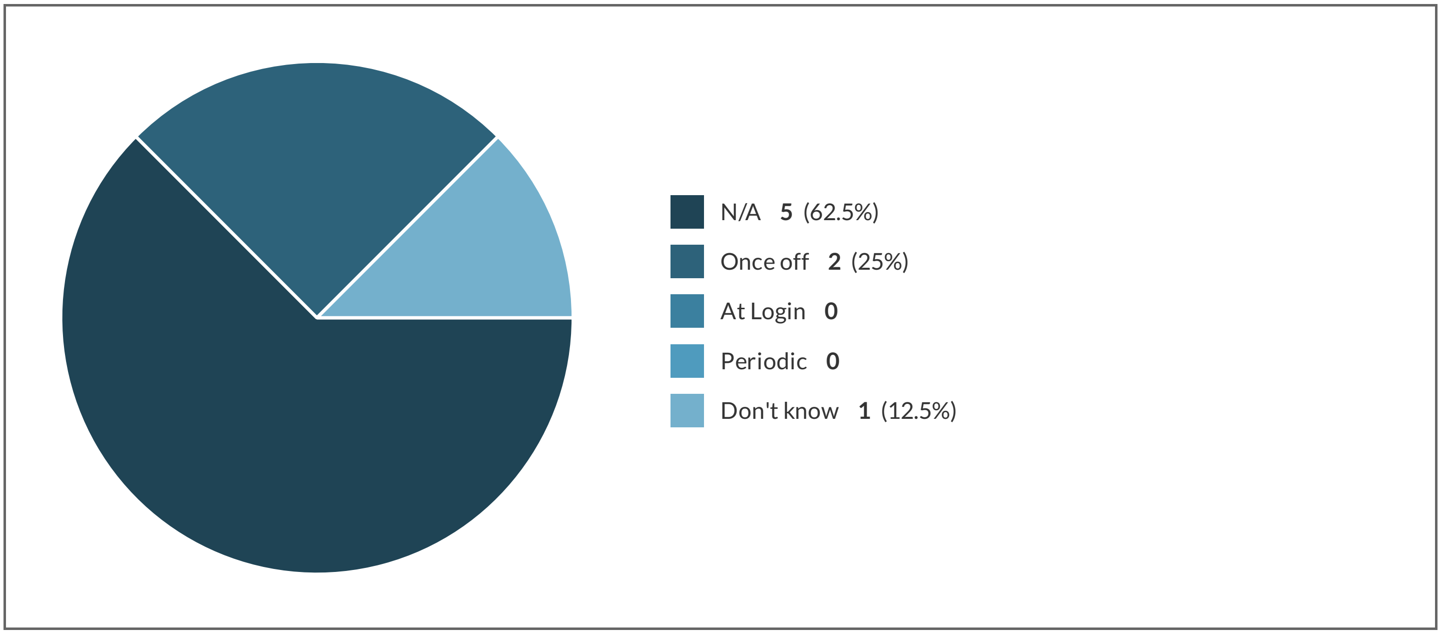


8.3 Organization needs extra resources

8.3.a Organization needs extra resources - Severity of Cost

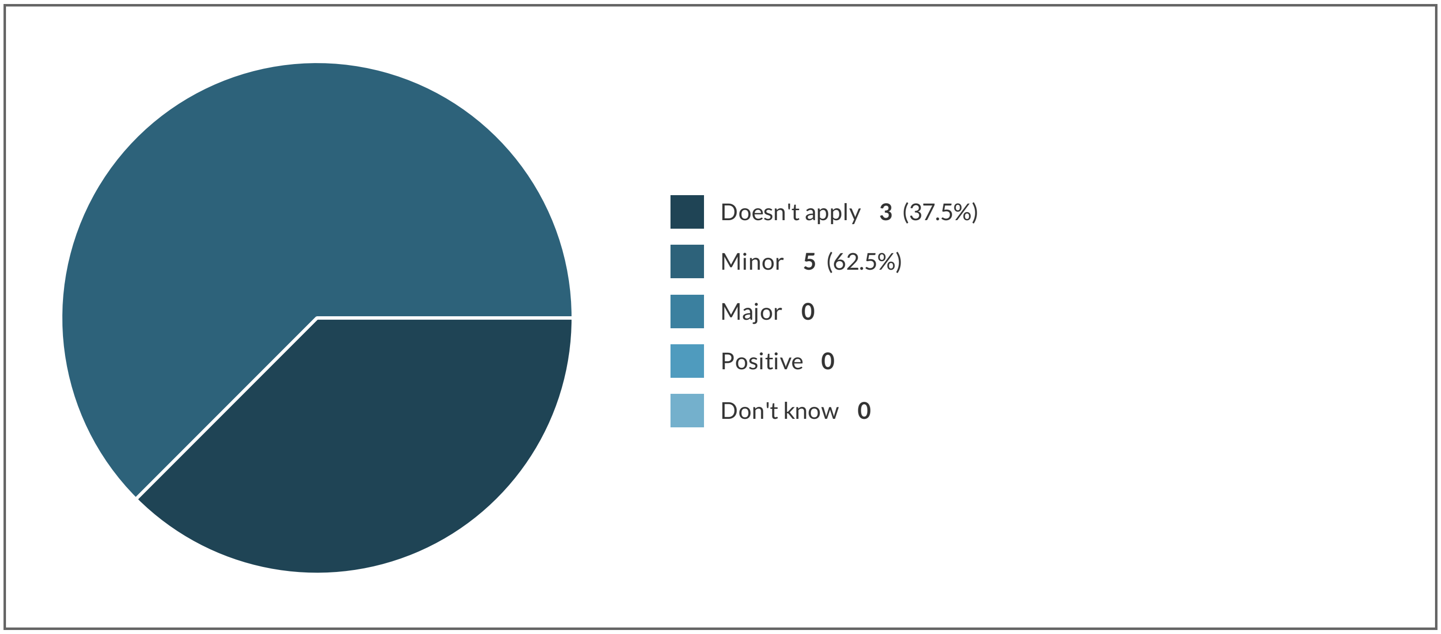


8.3.b Organization needs extra resources - Frequency Cost is Experienced

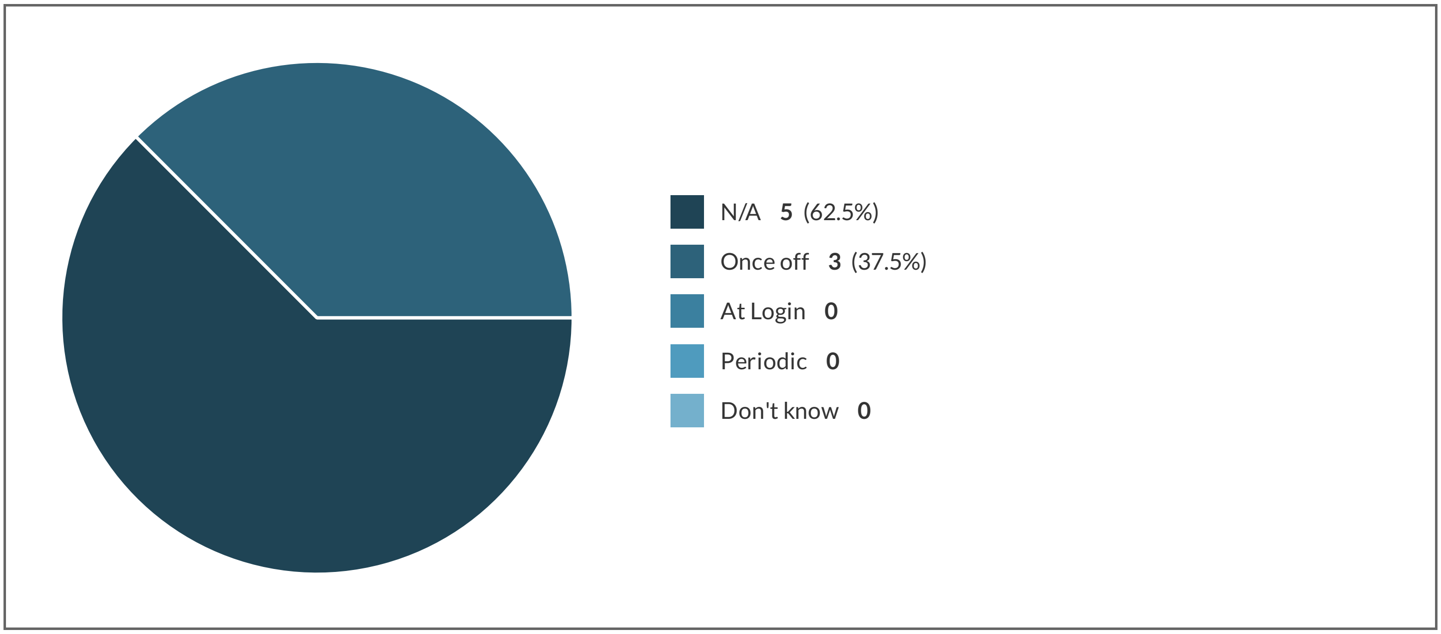


8.4 Takes organization time to implement

8.4.a Takes organization time to implement - Severity of Cost

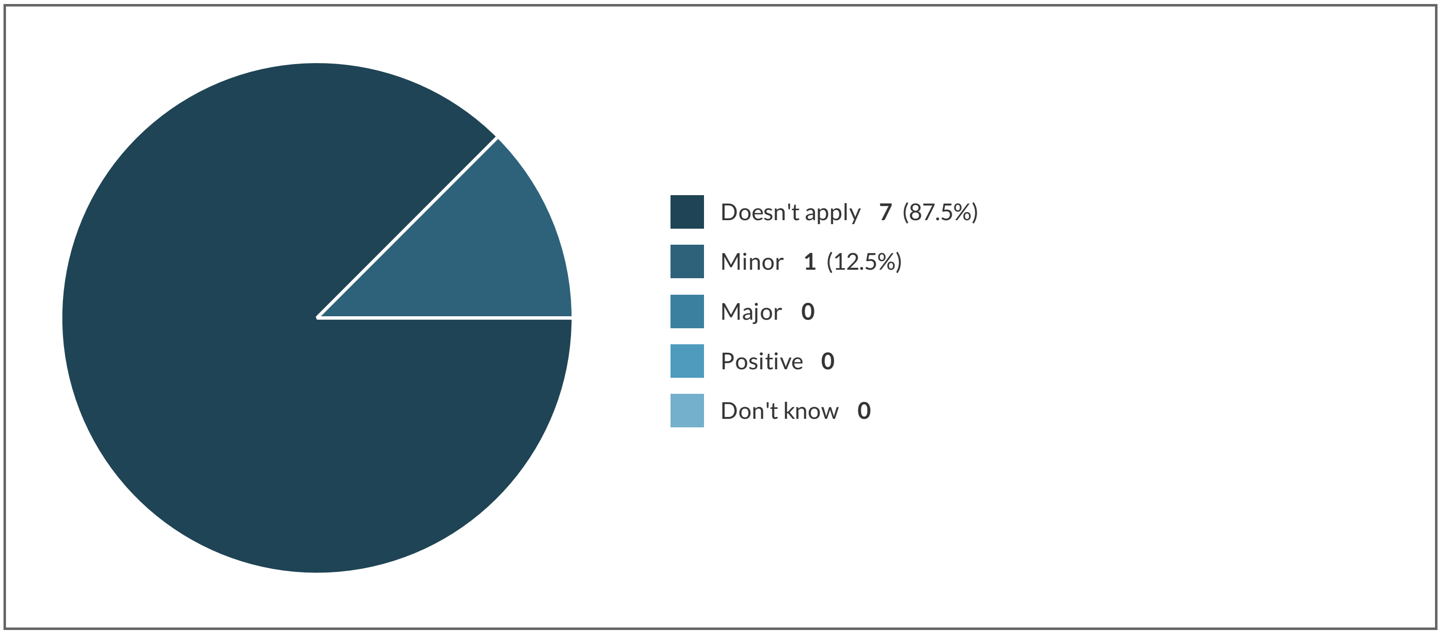


8.4.b Takes organization time to implement - Frequency Cost is Experienced

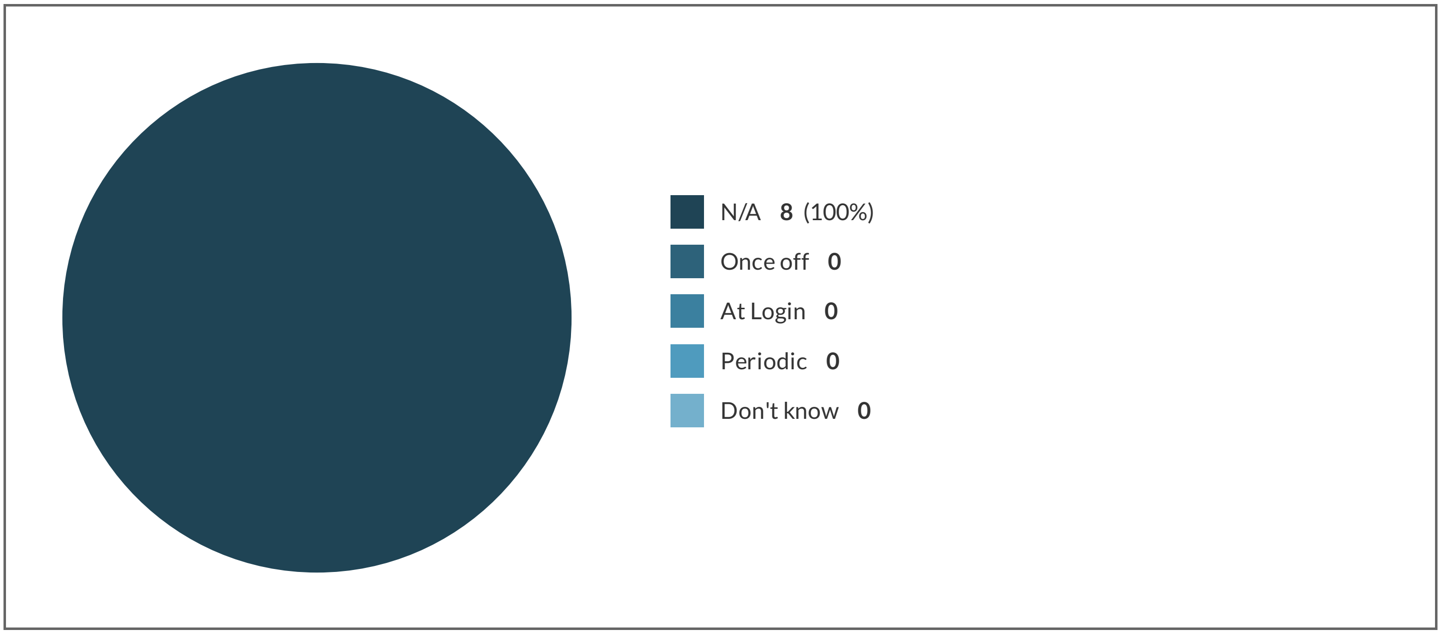


8.5 Increases the organization's computing power needed

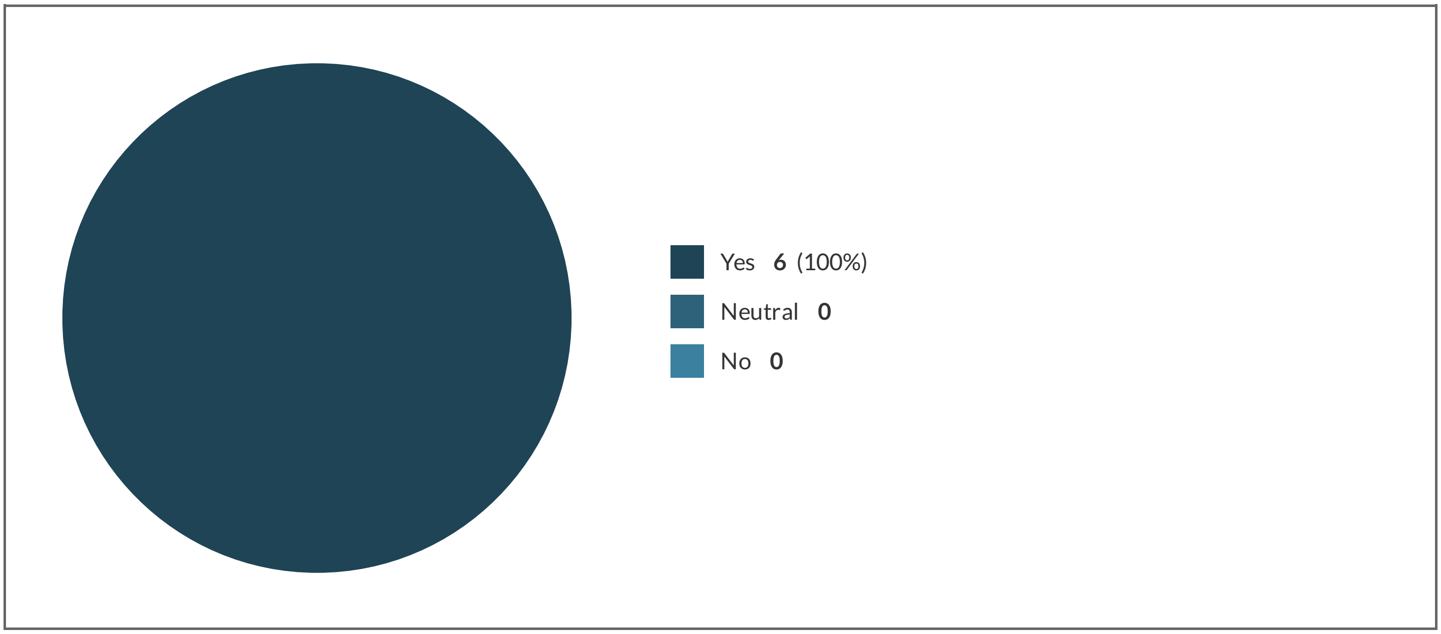
8.5.a Increases the organization's computing power needed - Severity of Cost



8.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



8.a Do you approve of this advice?



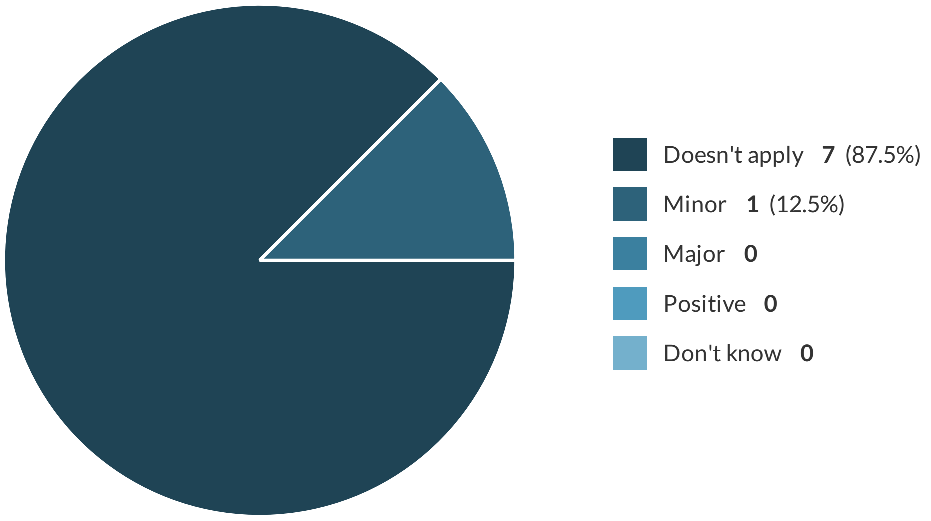
8.b Comments

Showing all 3 responses	
Passphrases make it easier for users to generate entropy, with some special characters, while still remembering their key is a better option than long string of gibberish that may lead to other security compromises and user frustration.	634211-634202-66090277
Again it hankers back to what we are setting up as a global multinational company who is probably a couple of years behind the leading edge when it comes to password rules	634211-634202-66754804
So to do this correctly users will need major education on how to correctly choose a password that is both memorable and secure. The longer a password is the harder the hash is to crack. For myself personally there is not a password in my "keychain" that is anything less than 16 characters (unless for some reason the thing I'm logging into has a max character requirement)	634211-634202-66754952

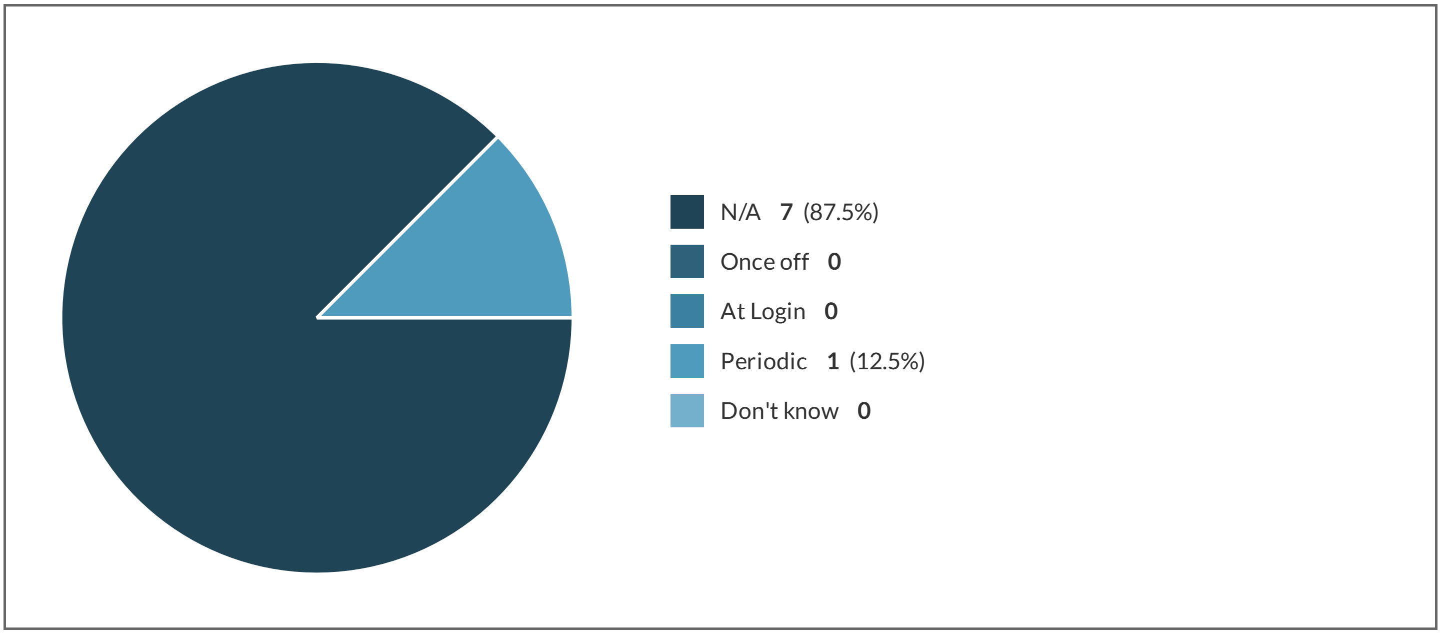
9 When logging in, users should not use the "remember me" option

9.1 Increased help desk/user support time

9.1.a Increased help desk/user support time - Severity of Cost

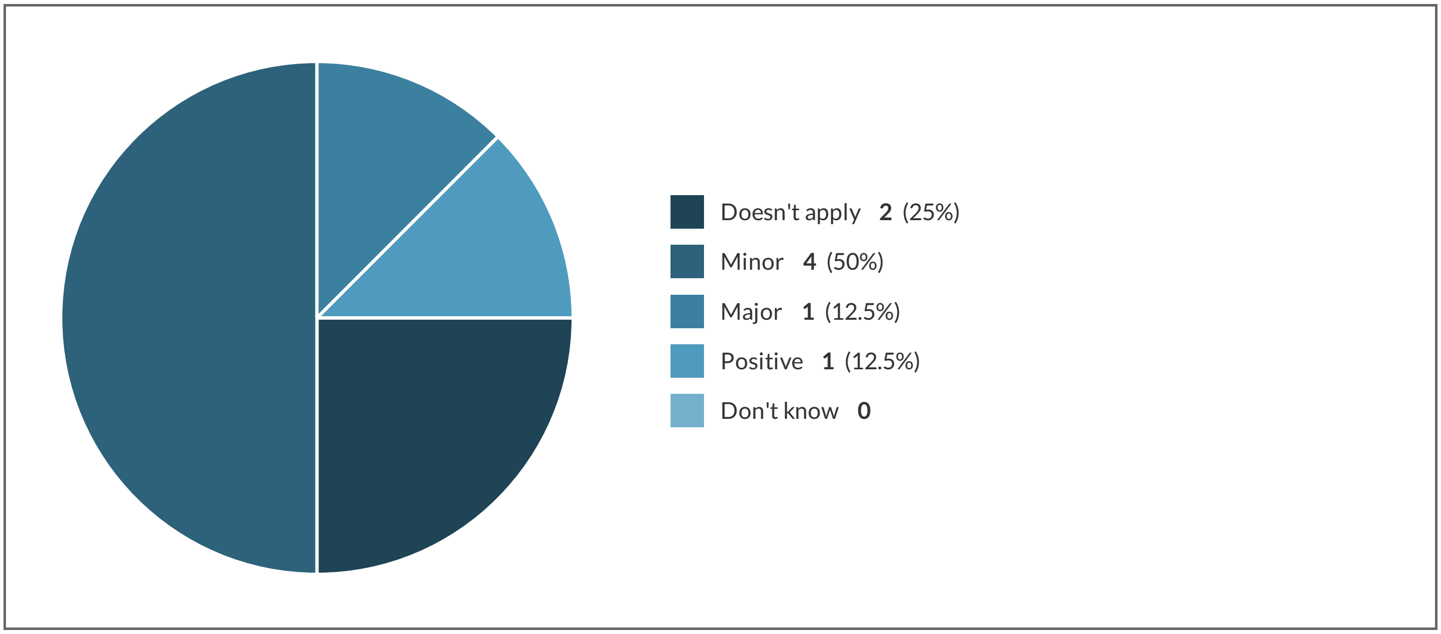


9.1.b Increased help desk/user support time - Frequency Cost is Experienced

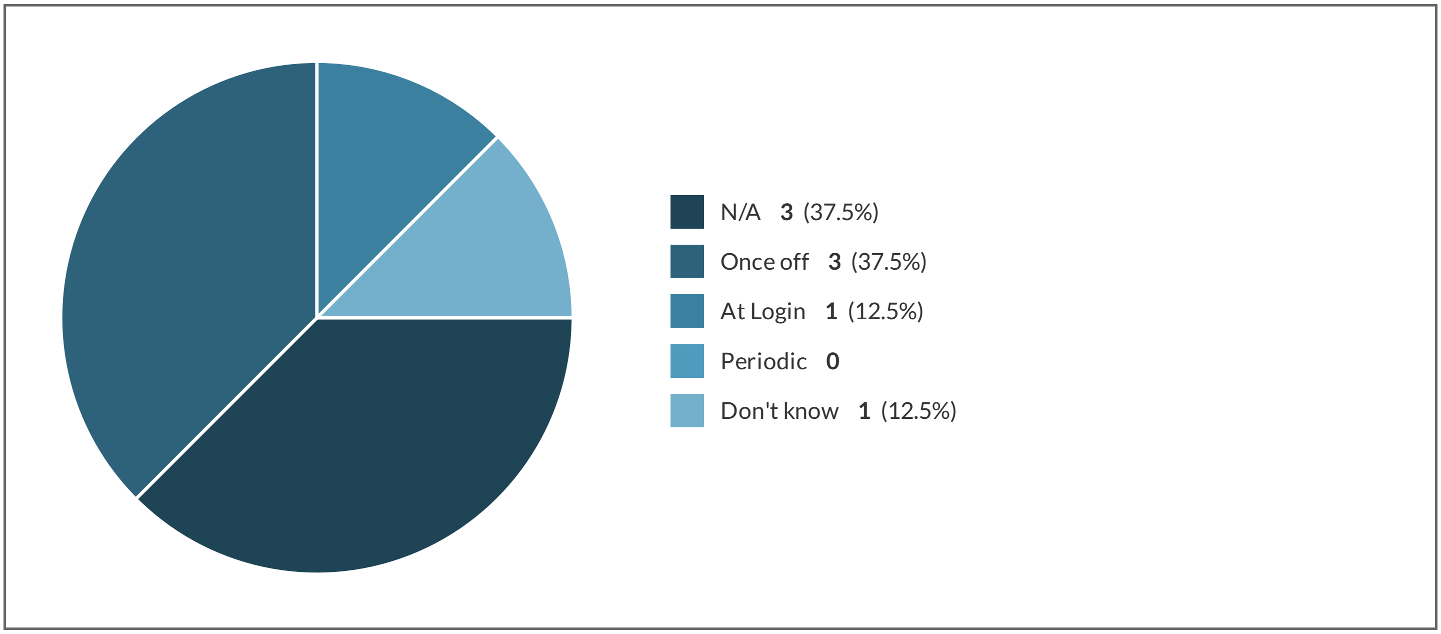


9.2 User education required

9.2.a User education required - Severity of Cost

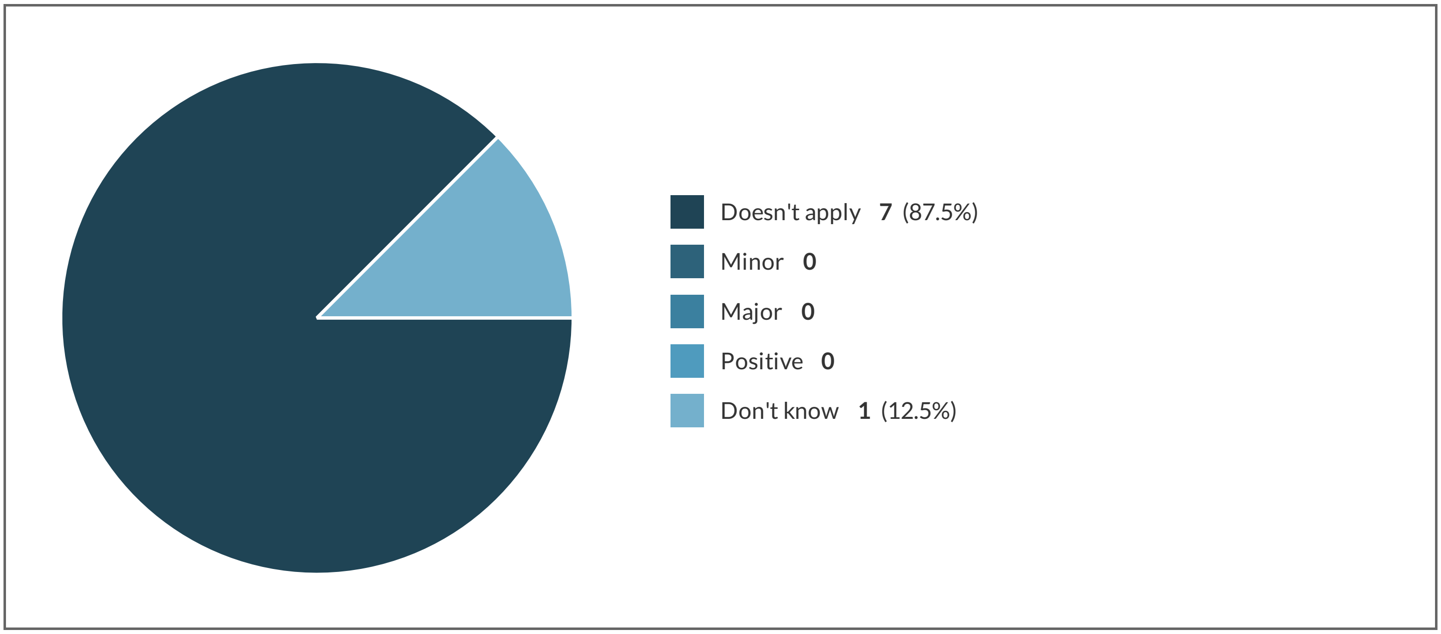


9.2.b User education required - Frequency Cost is Experienced

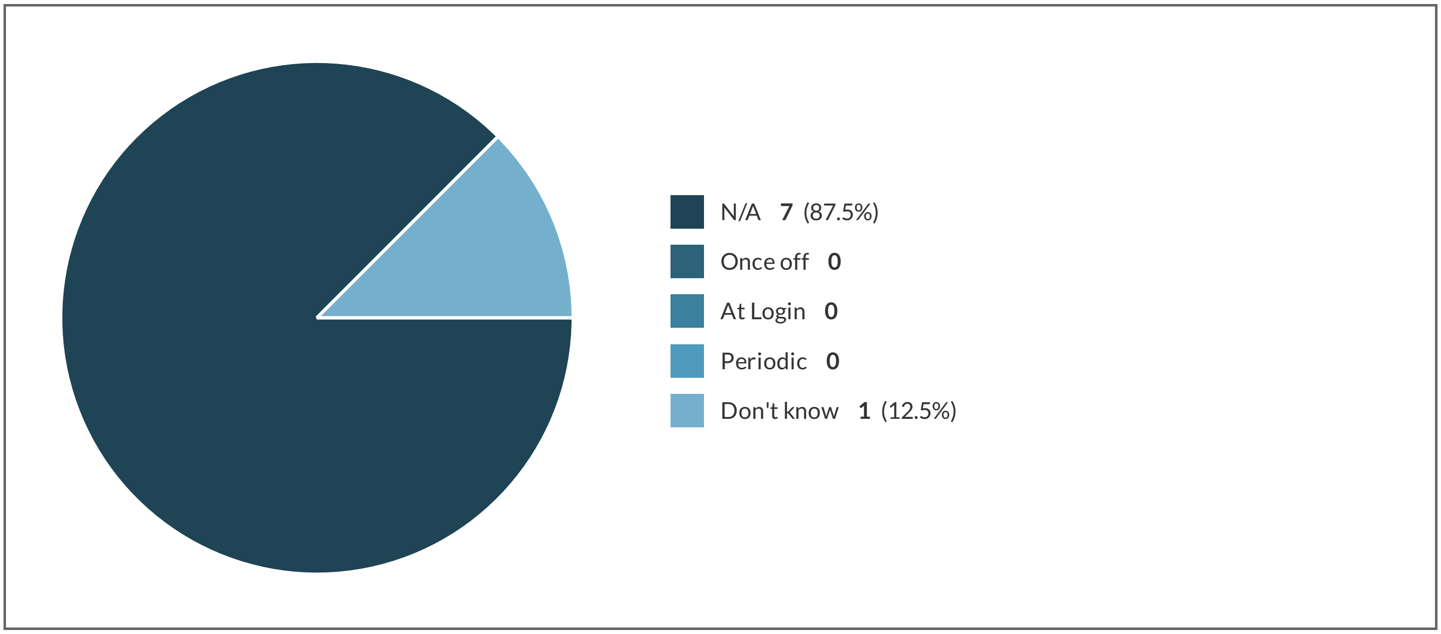


9.3 Organization needs extra resources

9.3.a Organization needs extra resources - Severity of Cost

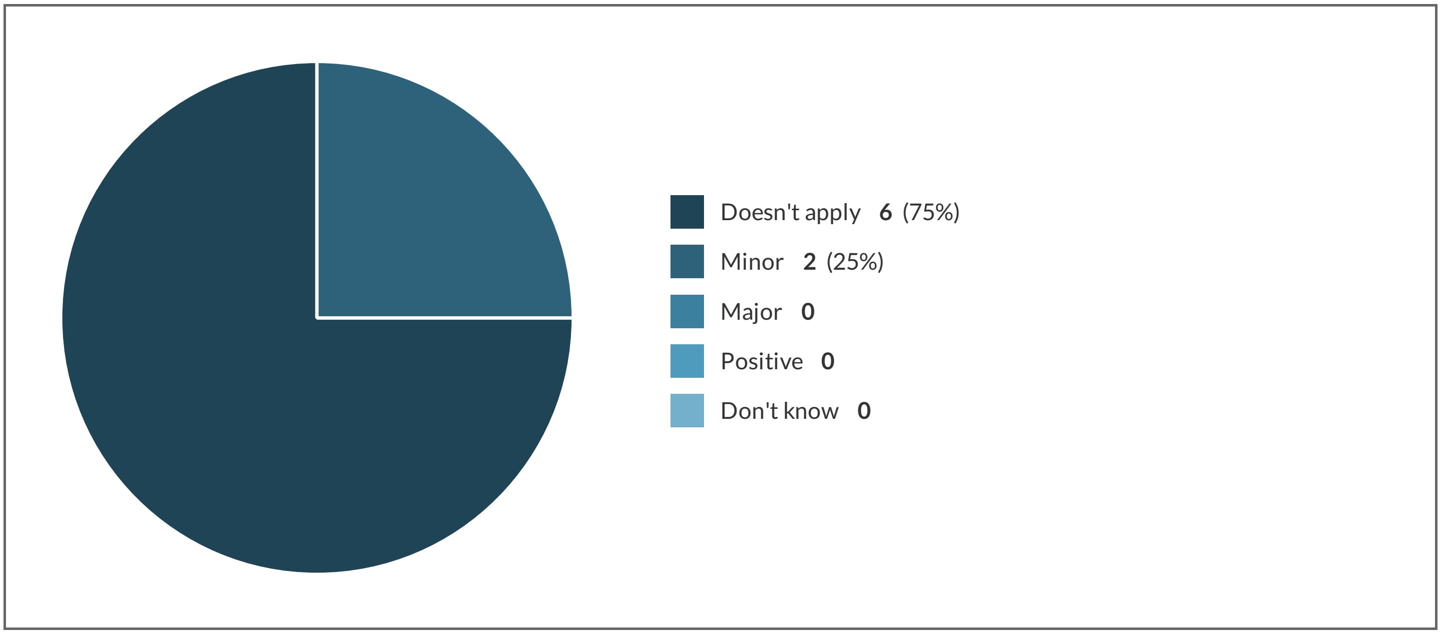


9.3.b Organization needs extra resources - Frequency Cost is Experienced

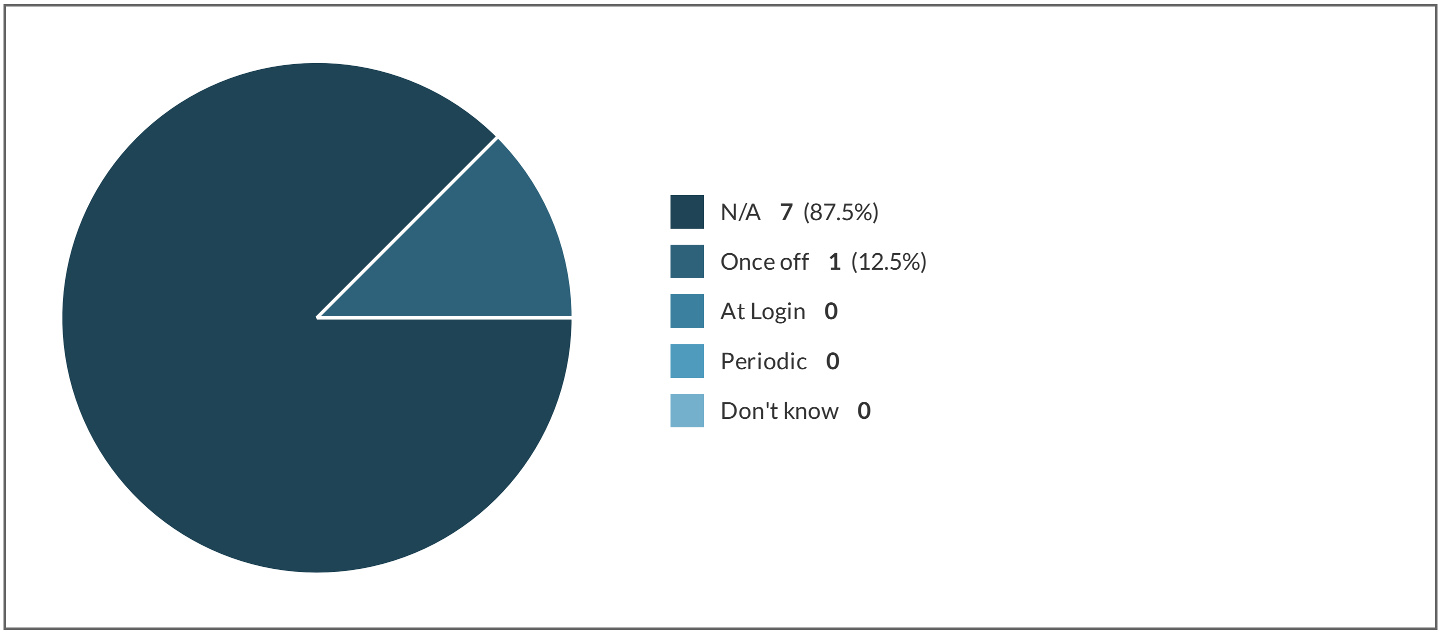


9.4 Takes organization time to implement

9.4.a Takes organization time to implement - Severity of Cost

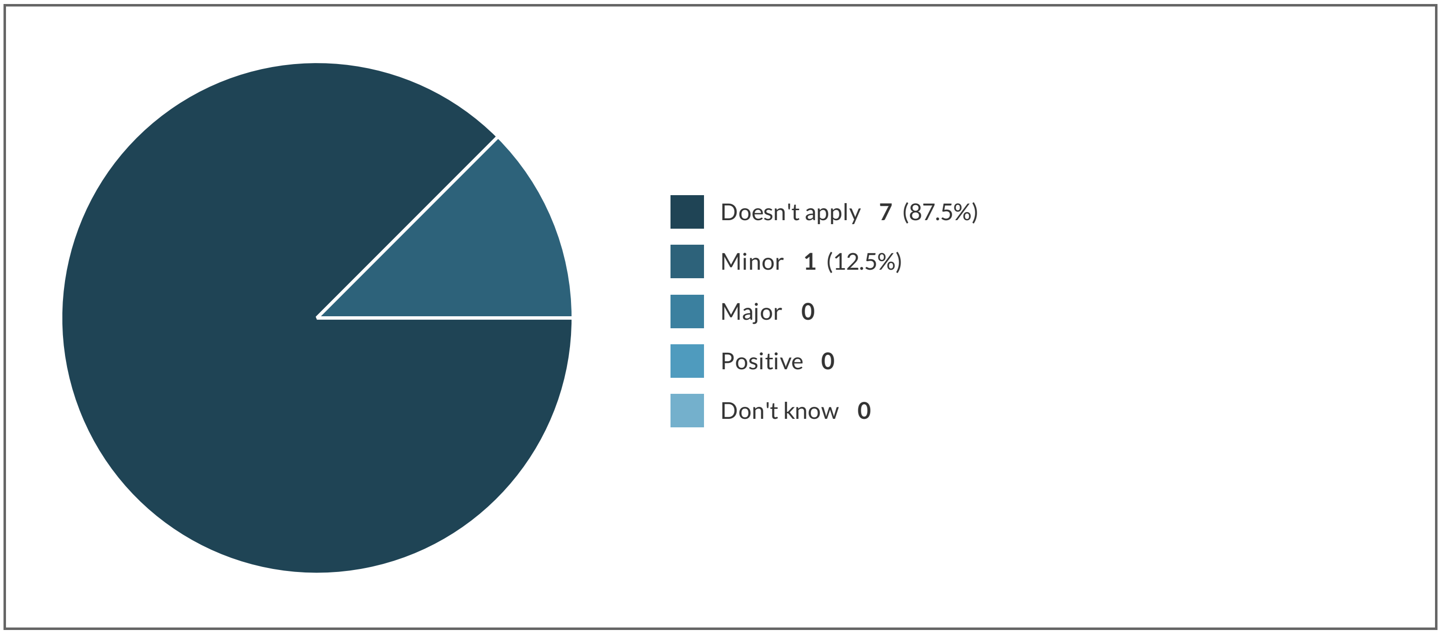


9.4.b Takes organization time to implement - Frequency Cost is Experienced

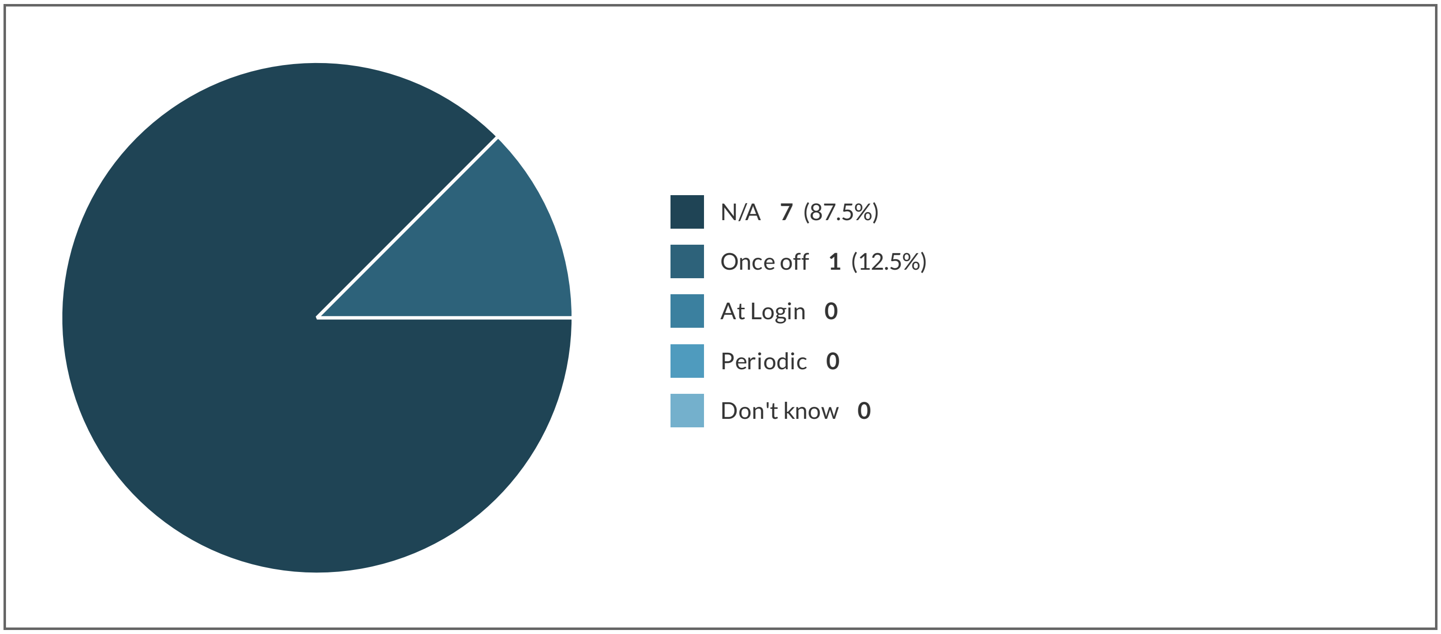


9.5 Increases the organization's computing power needed

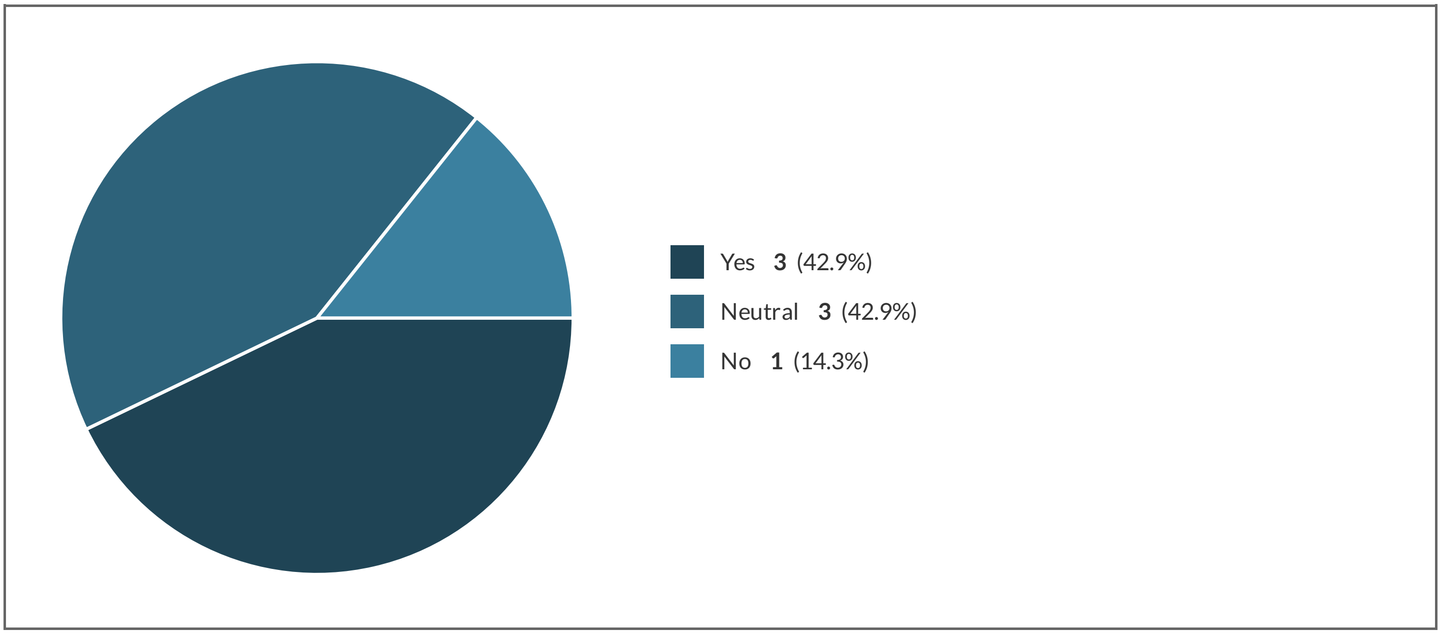
9.5.a Increases the organization's computing power needed - Severity of Cost



9.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



9.a Do you approve of this advice?



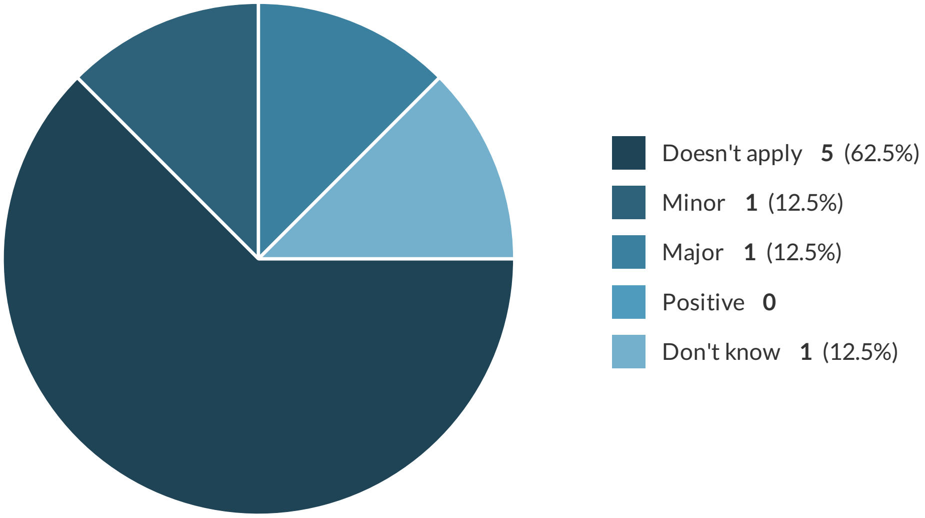
9.b Comments

Showing all 5 responses	
Assuming this past the primary device login stage	634211-634202-66090277
if the system is secure and only one user, its not minded	634211-634202-66098698
Users should use a password manager	634211-634202-66532254
Laptops can get stolen, people can come up to work stations when they are empty.	634211-634202-66754952
Absolutely	634211-634202-66871889

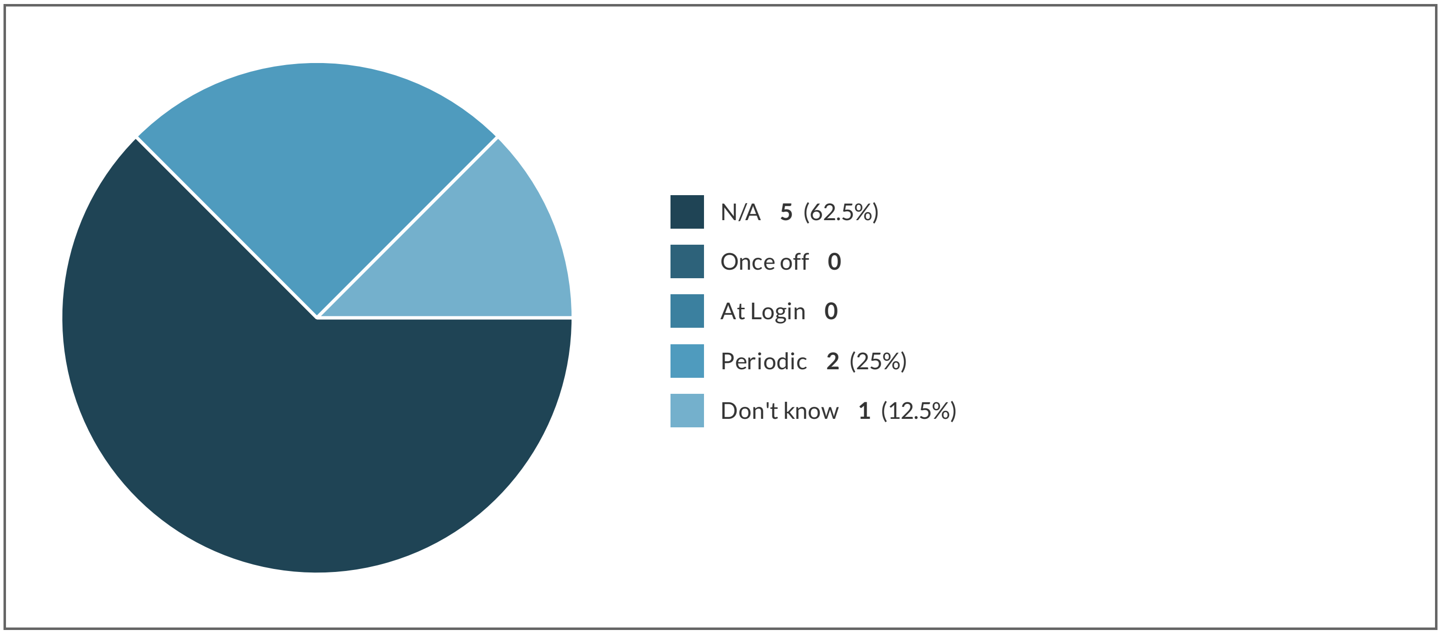
10 A user should never send their password by email

10.1 Increased help desk/user support time

10.1.a Increased help desk/user support time - Severity of Cost

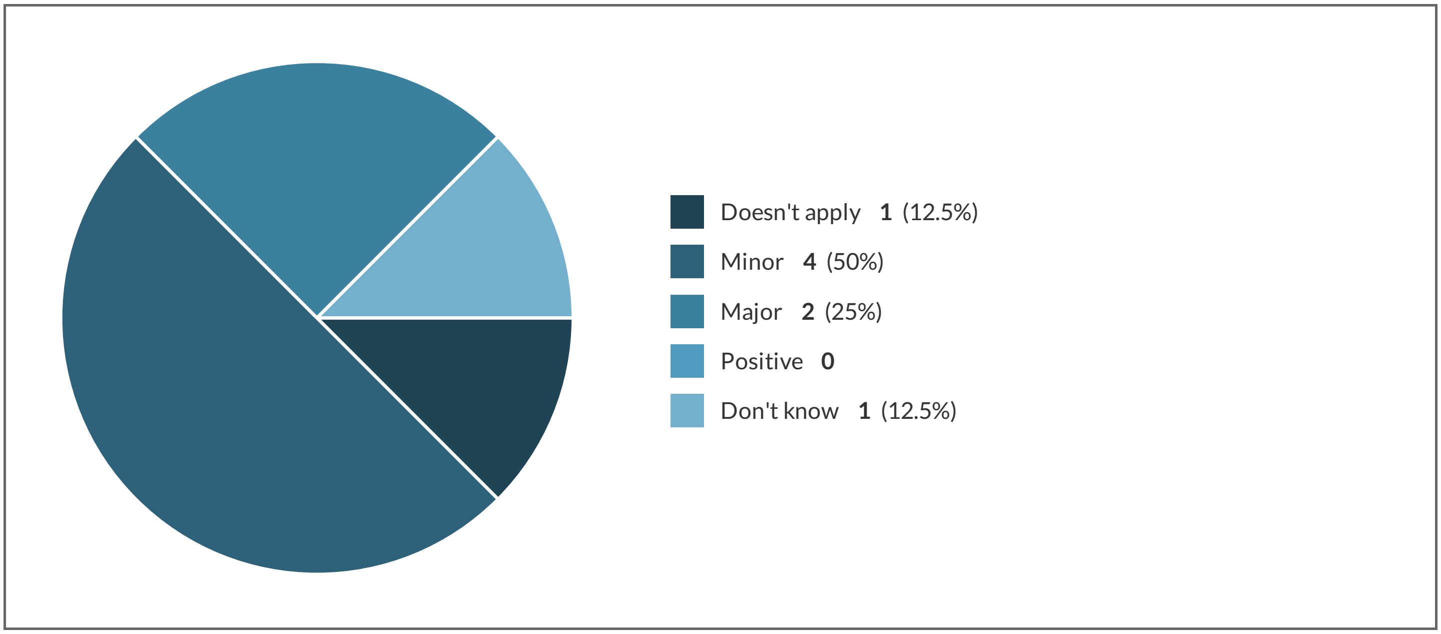


10.1.b Increased help desk/user support time - Frequency Cost is Experienced

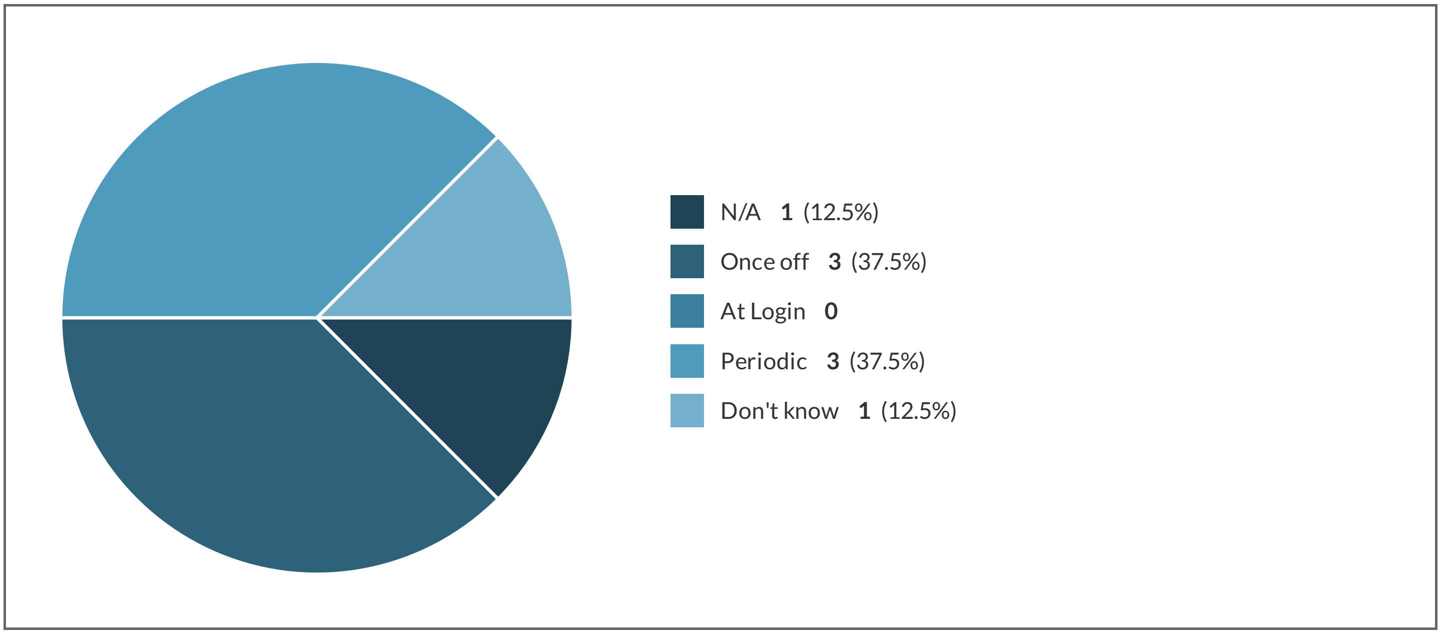


10.2 User education required

10.2.a User education required - Severity of Cost

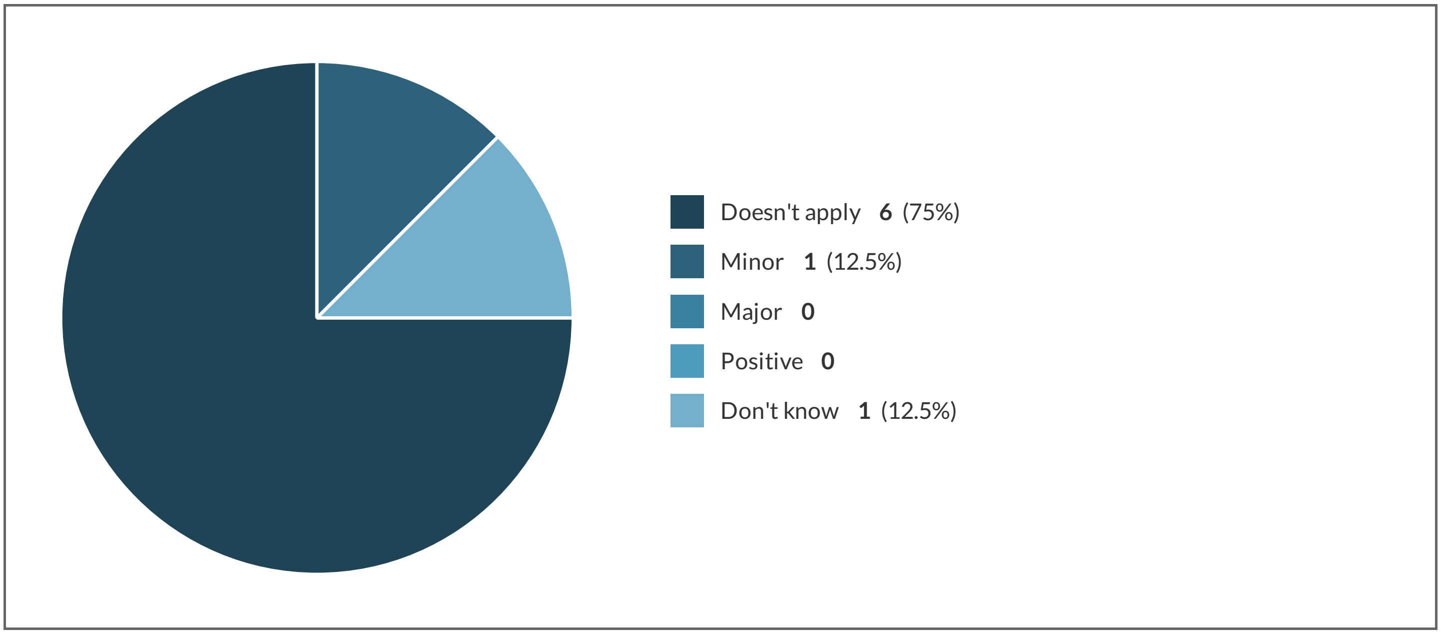


10.2.b User education required - Frequency Cost is Experienced

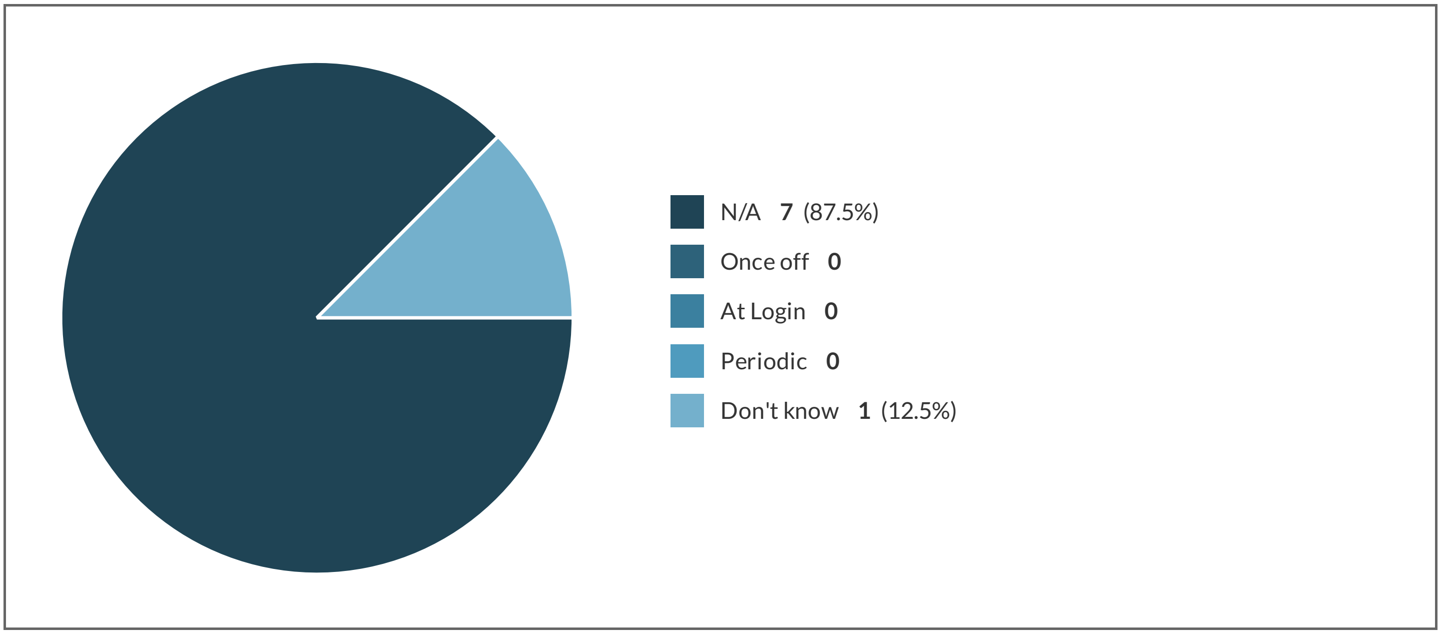


10.3 Organization needs extra resources

10.3.a Organization needs extra resources - Severity of Cost

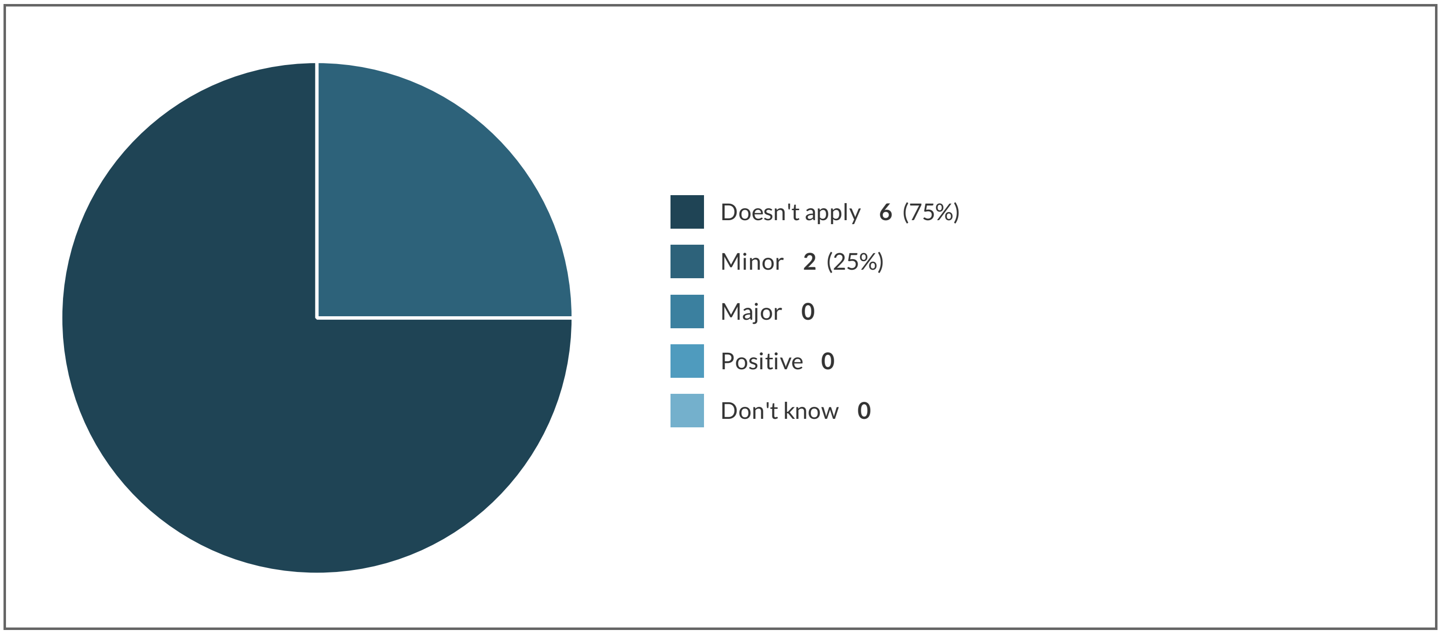


10.3.b Organization needs extra resources - Frequency Cost is Experienced

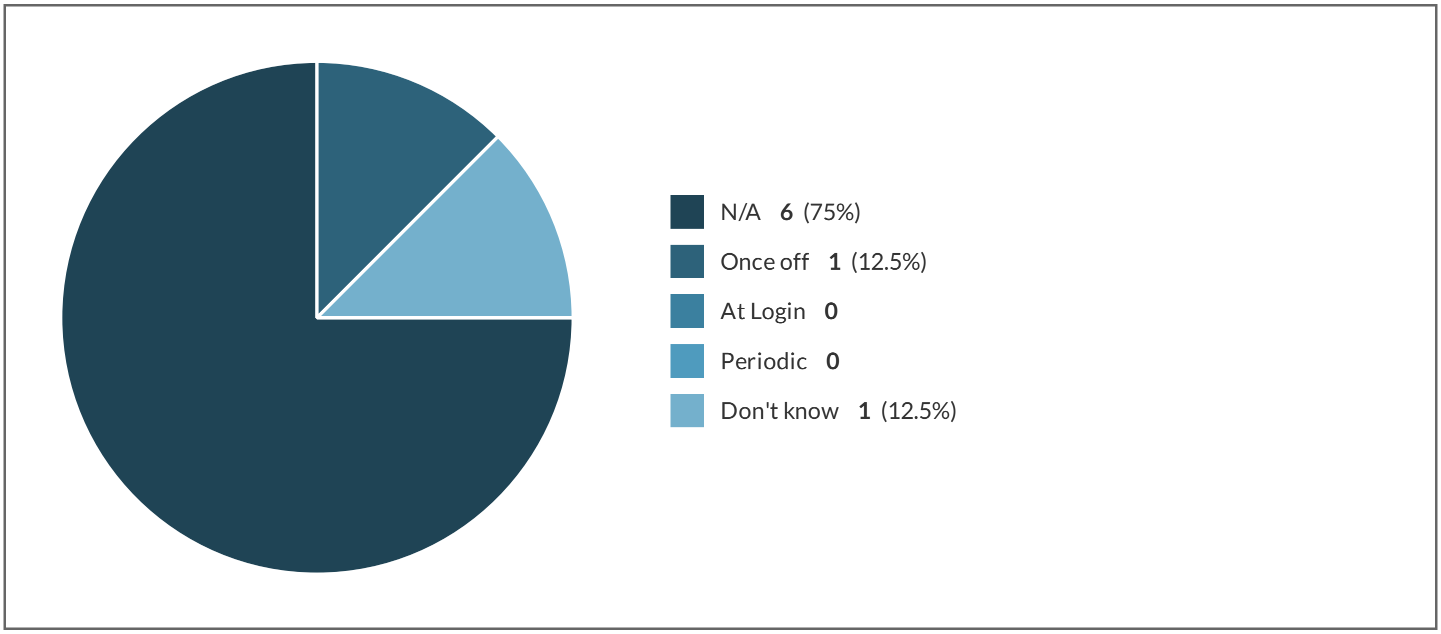


10.4 Takes organization time to implement

10.4.a Takes organization time to implement - Severity of Cost

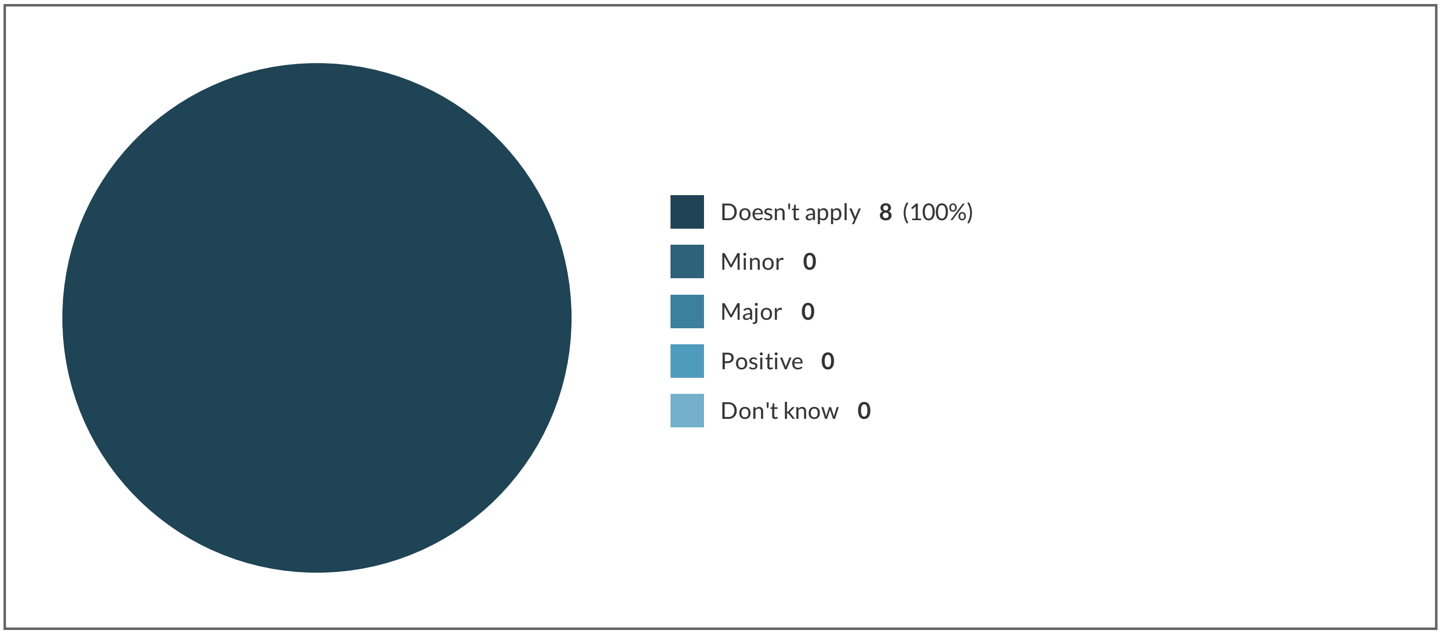


10.4.b Takes organization time to implement - Frequency Cost is Experienced

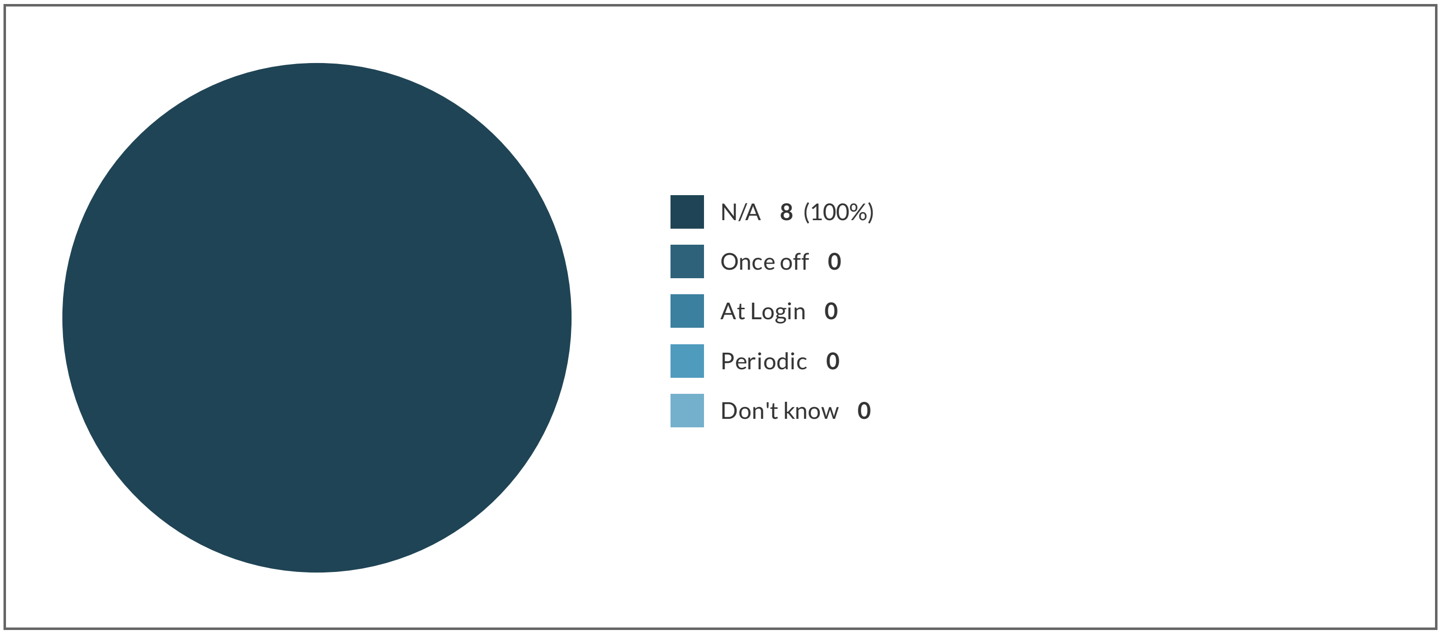


10.5 Increases the organization's computing power needed

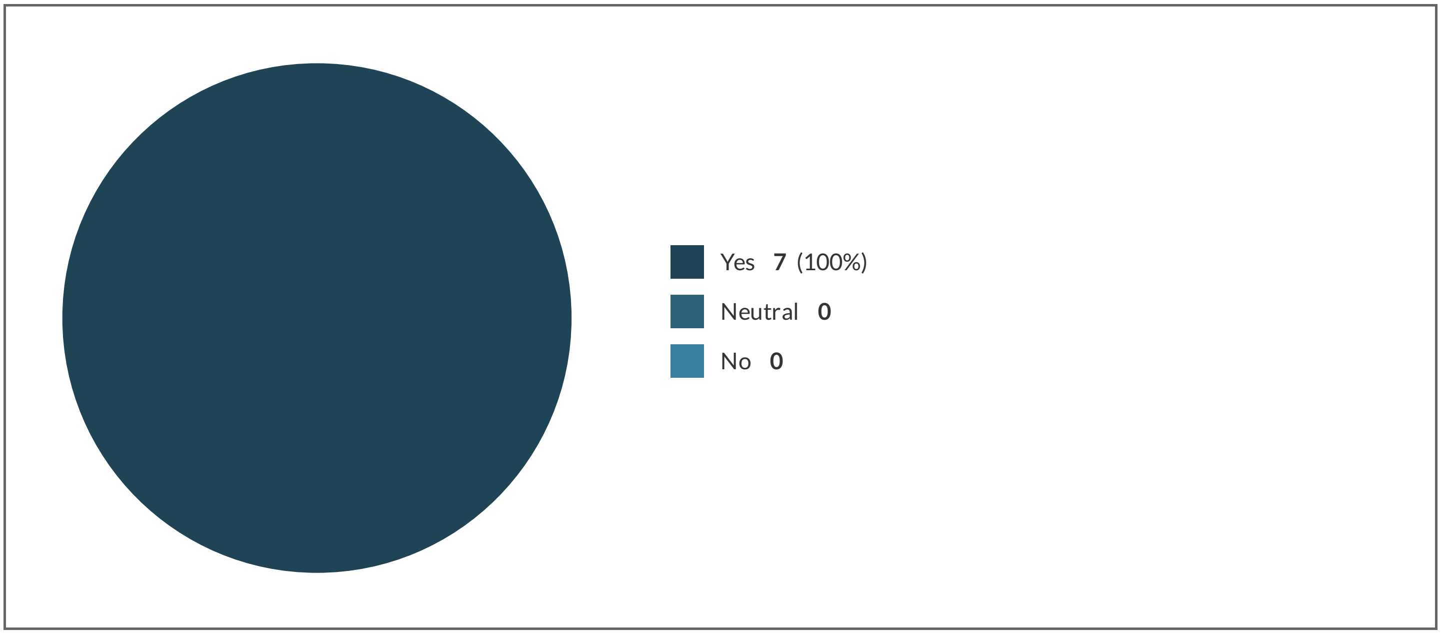
10.5.a Increases the organization's computing power needed - Severity of Cost



10.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



10.a Do you approve of this advice?



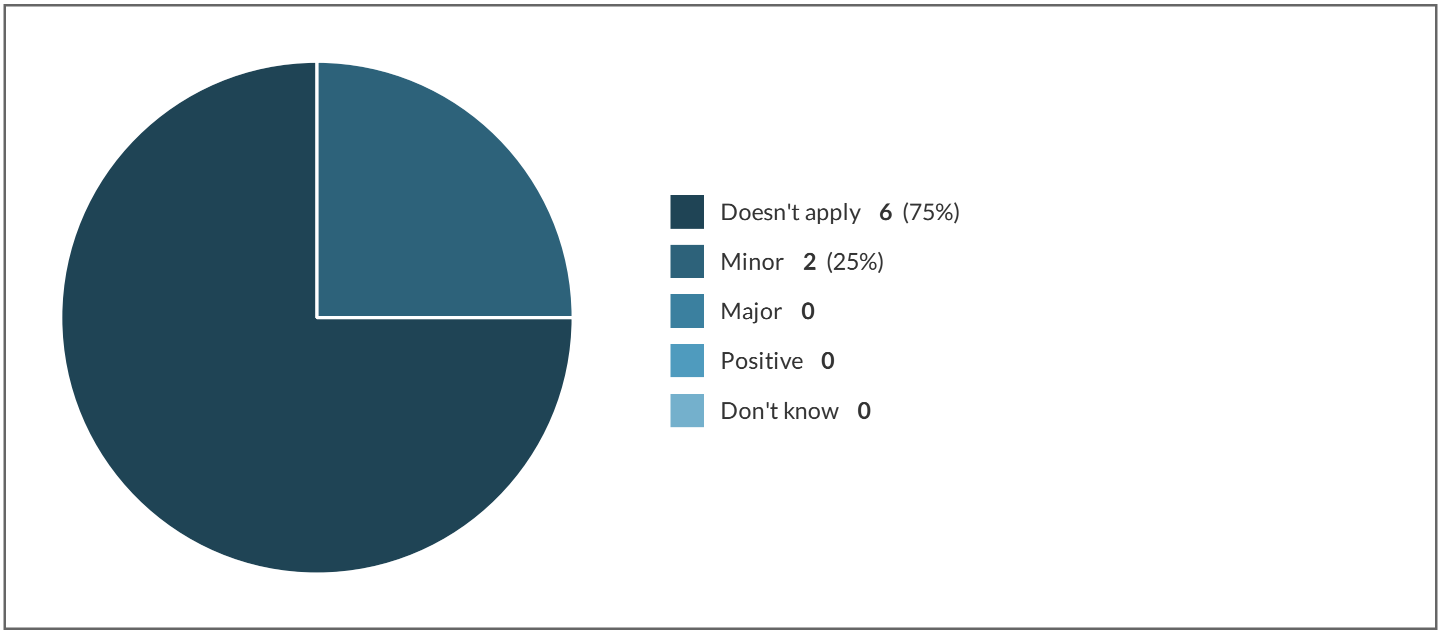
10.b Comments

Showing all 5 responses	
Users are the week link - don't waste time trying to do anything but education here.	634211-634202-66090277
the expense is in the afterward..	634211-634202-66098698
There needs to be a better method for sharing passwords with either onsite tech support or policy's in place to support	634211-634202-66754804
I would extend that to say that passwords should never be written down or stored digitally anywhere. With the only exception to that rule being whilst using a password manager like LastPass or OnePassword	634211-634202-66754952
Absolutely	634211-634202-66871889

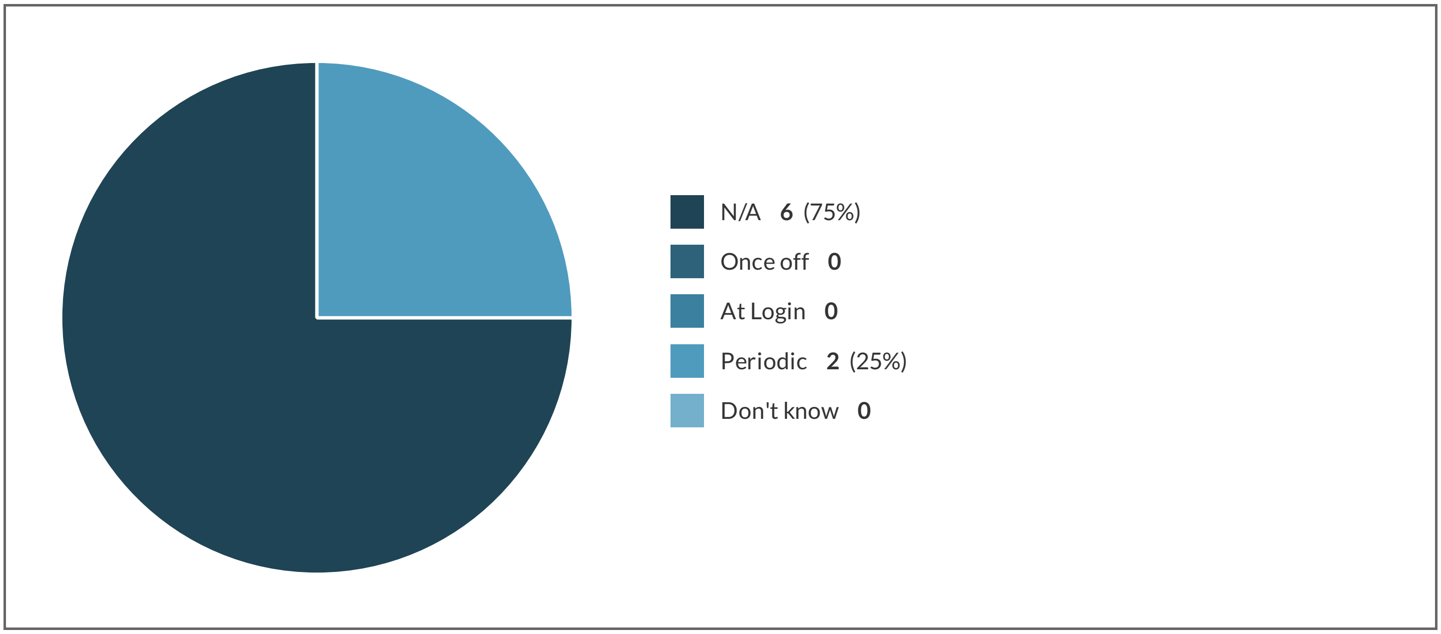
11 A user's email should be kept up-to-date and secure

11.1 Increased help desk/user support time

11.1.a Increased help desk/user support time - Severity of Cost

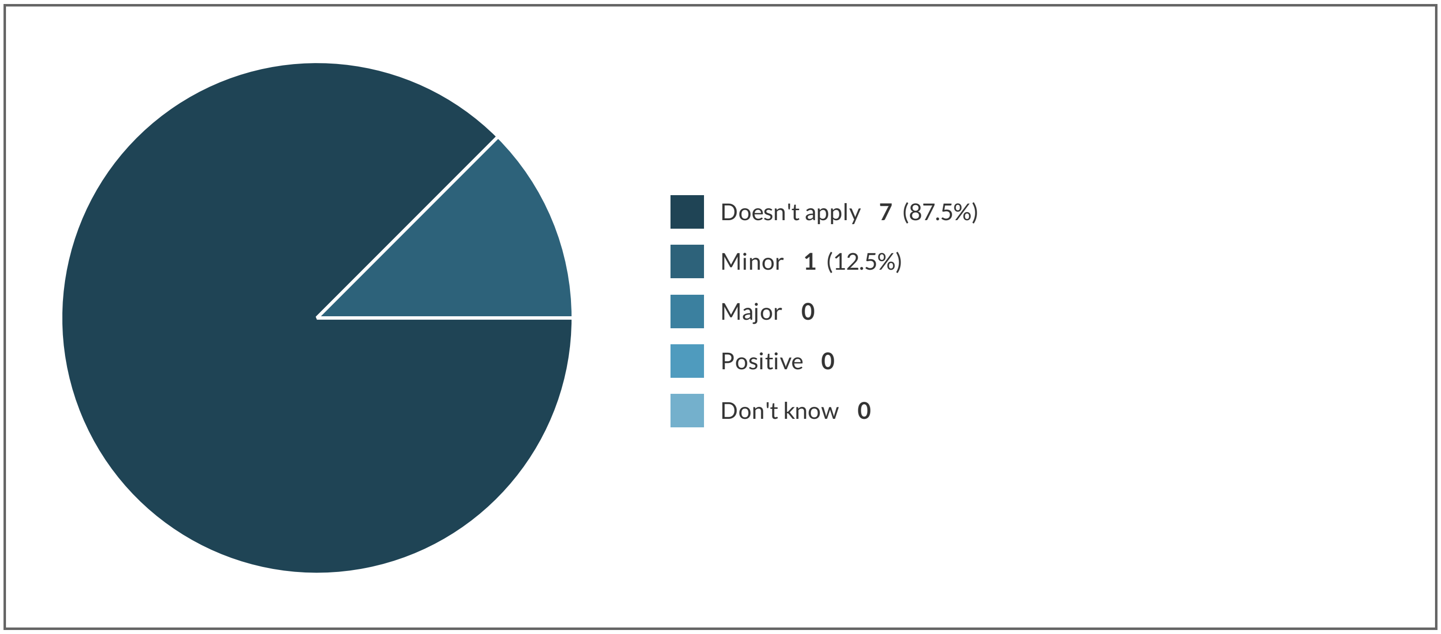


11.1.b Increased help desk/user support time - Frequency Cost is Experienced

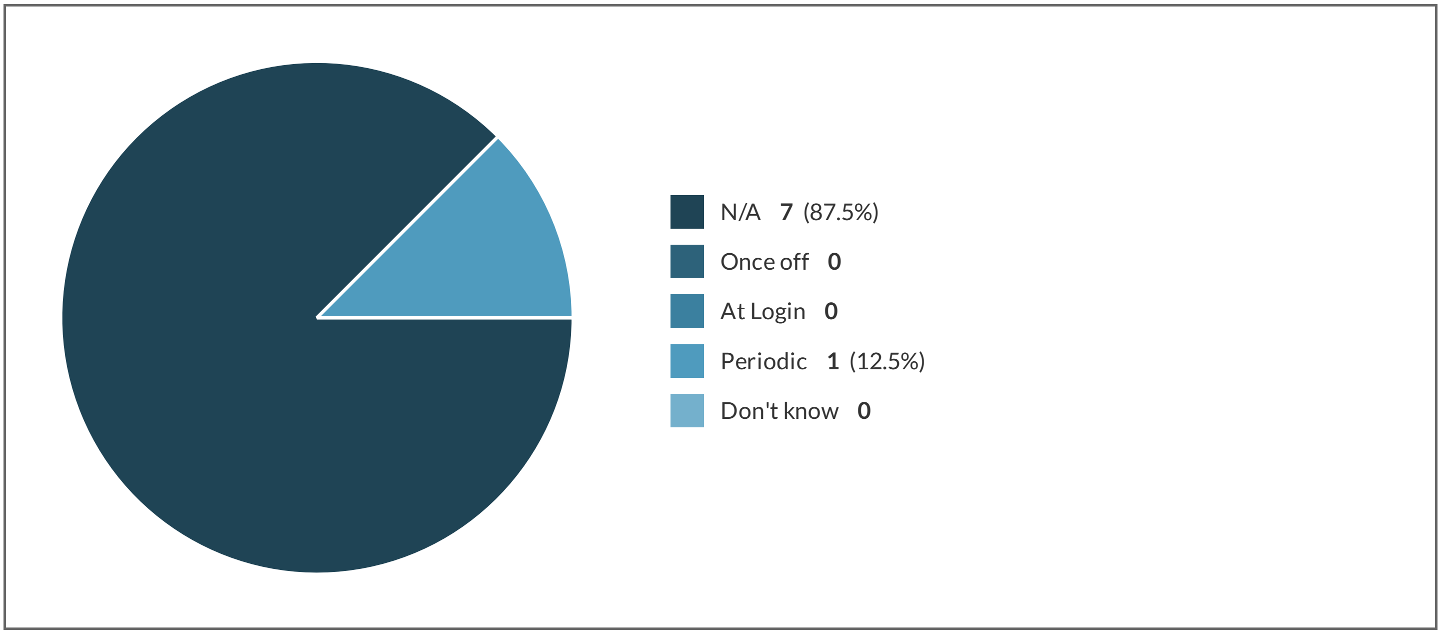


11.2 User education required

11.2.a User education required - Severity of Cost

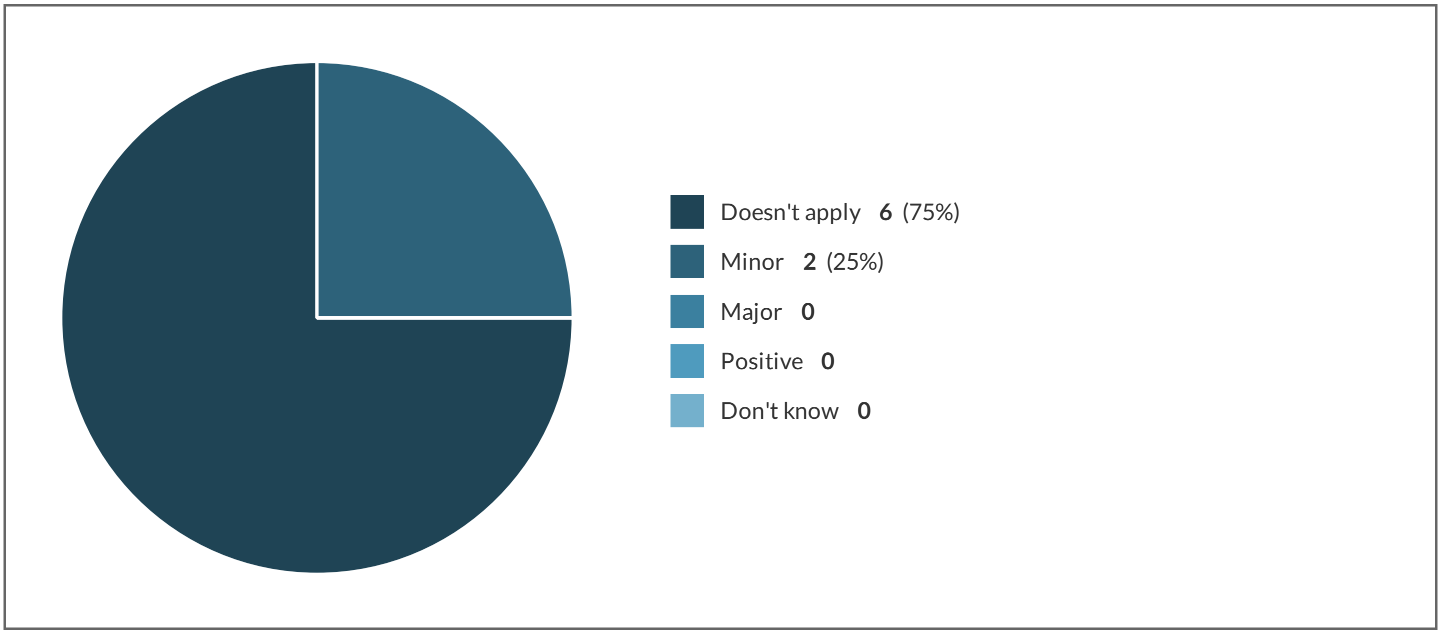


11.2.b User education required - Frequency Cost is Experienced

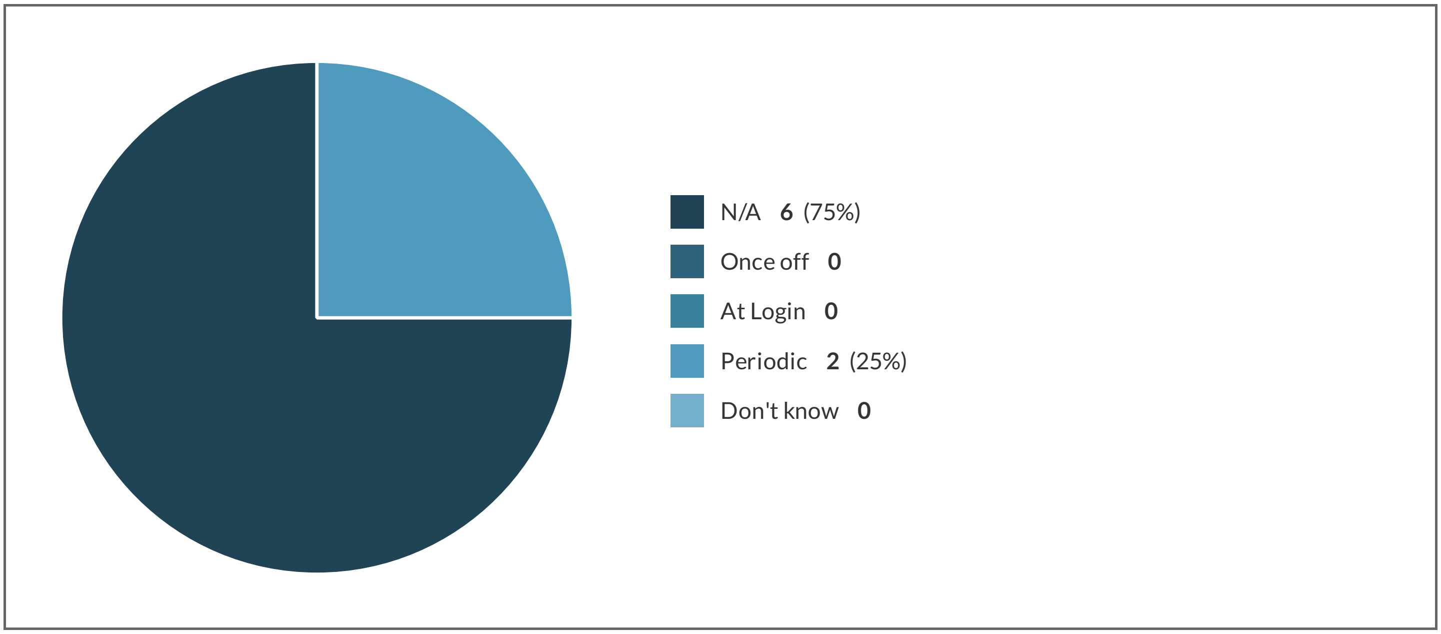


11.3 Organization needs extra resources

11.3.a Organization needs extra resources - Severity of Cost

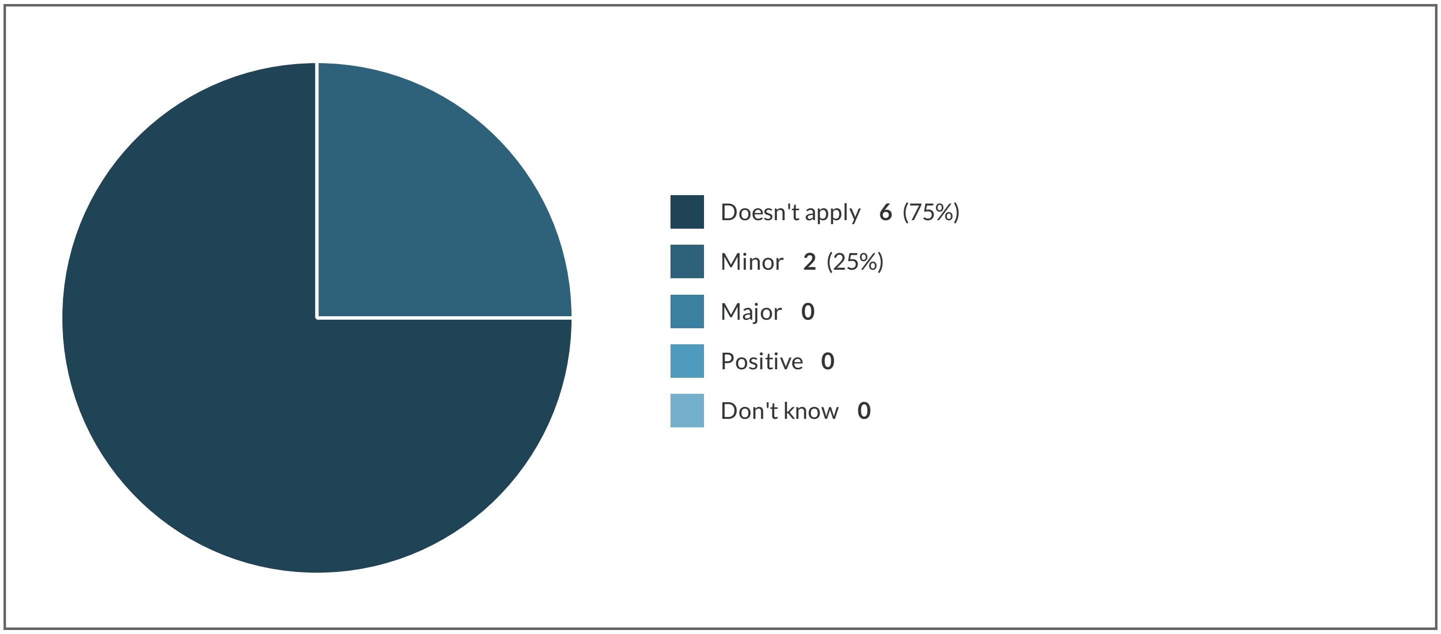


11.3.b Organization needs extra resources - Frequency Cost is Experienced

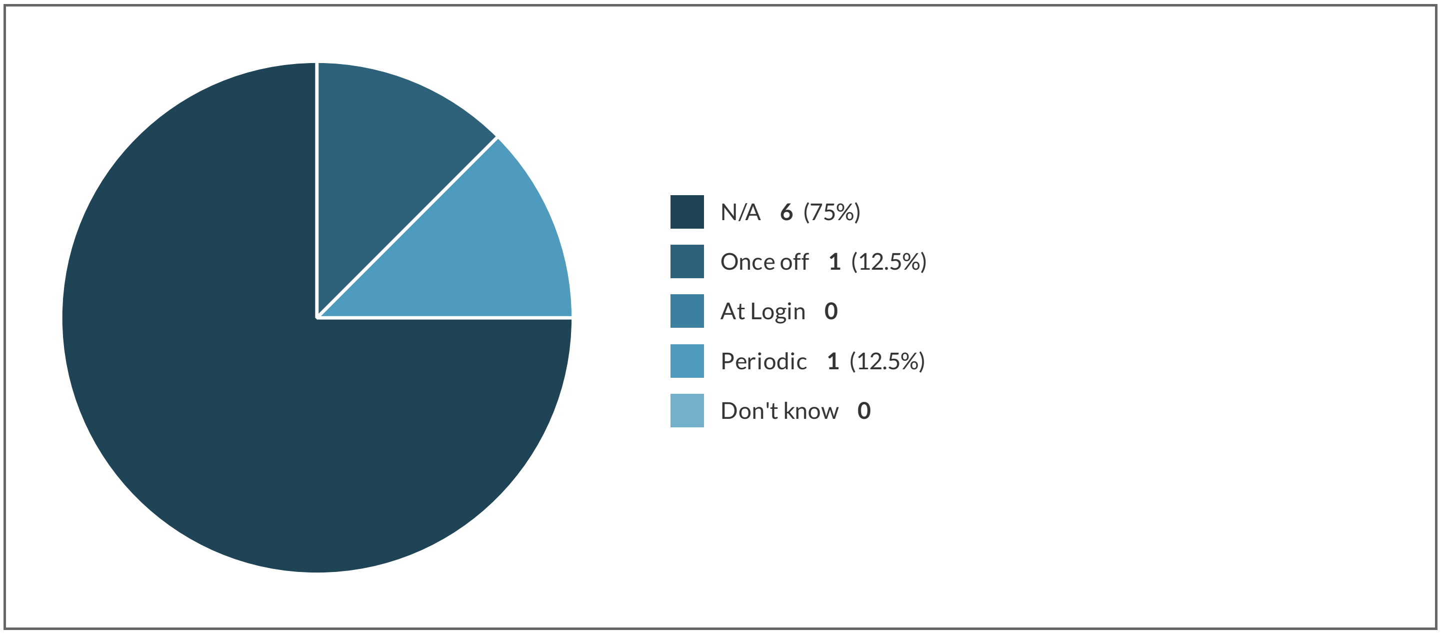


11.4 Takes organization time to implement

11.4.a Takes organization time to implement - Severity of Cost

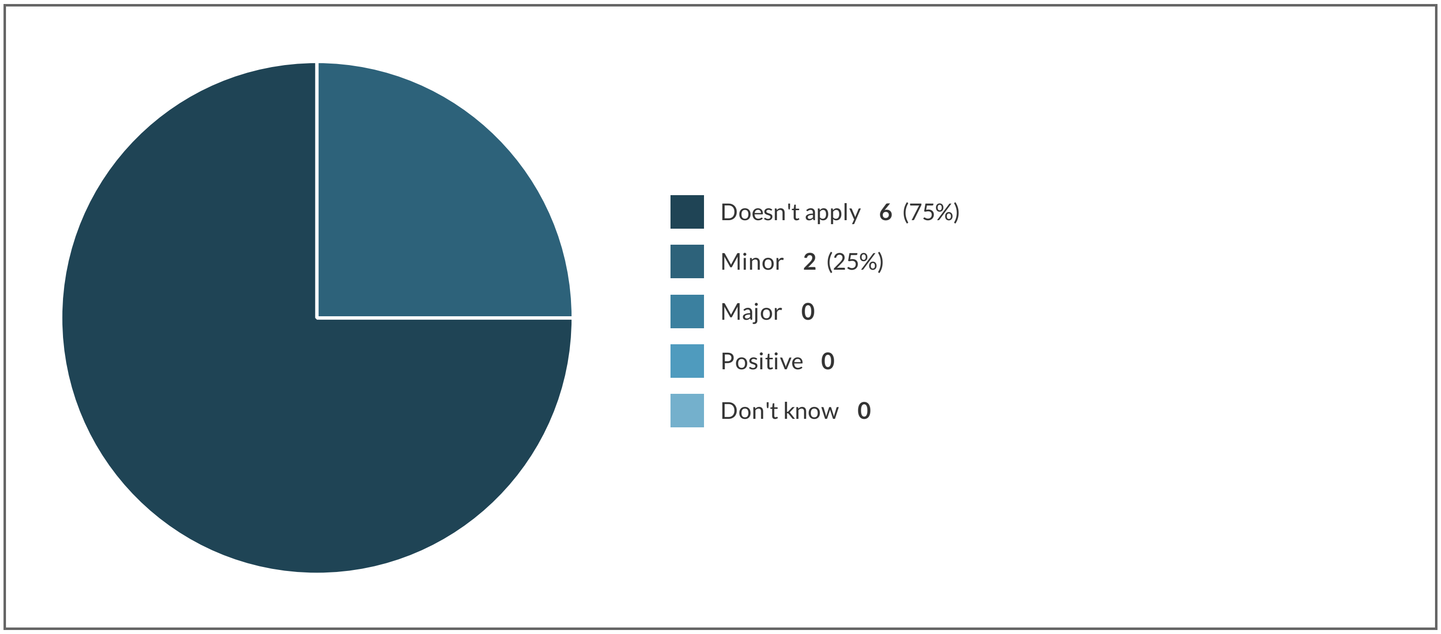


11.4.b Takes organization time to implement - Frequency Cost is Experienced

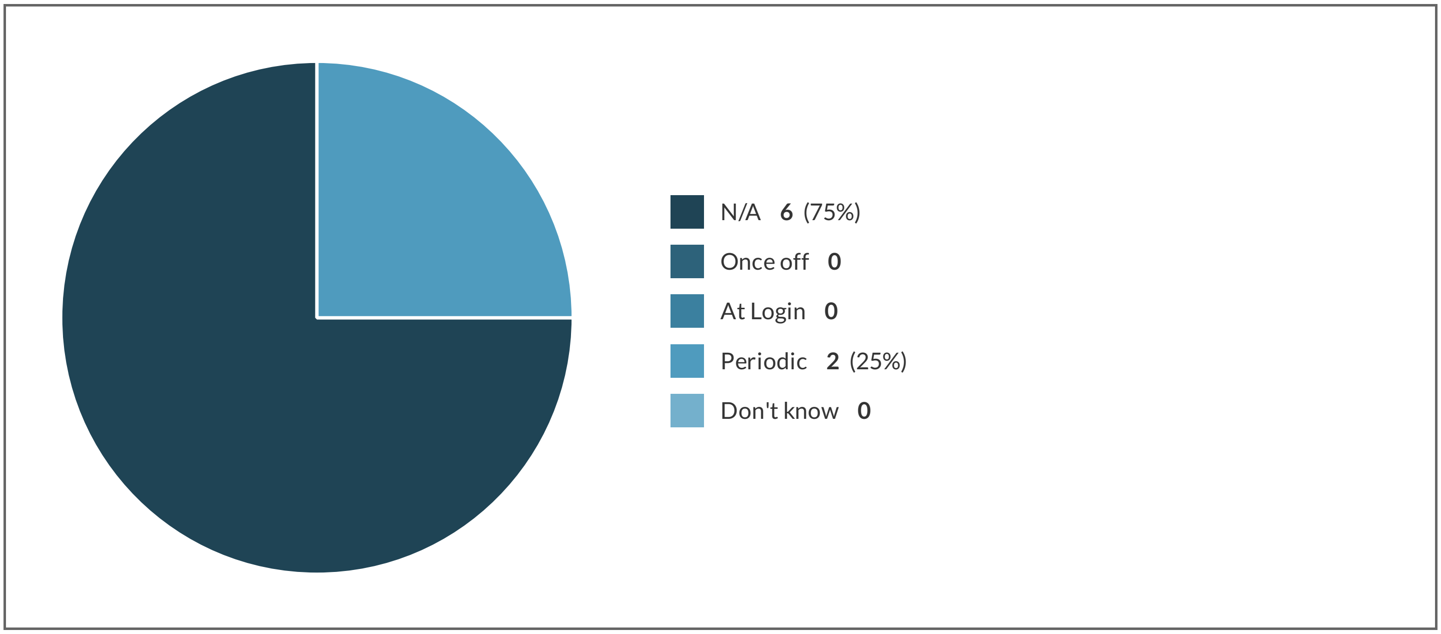


11.5 Increases the organization's computing power needed

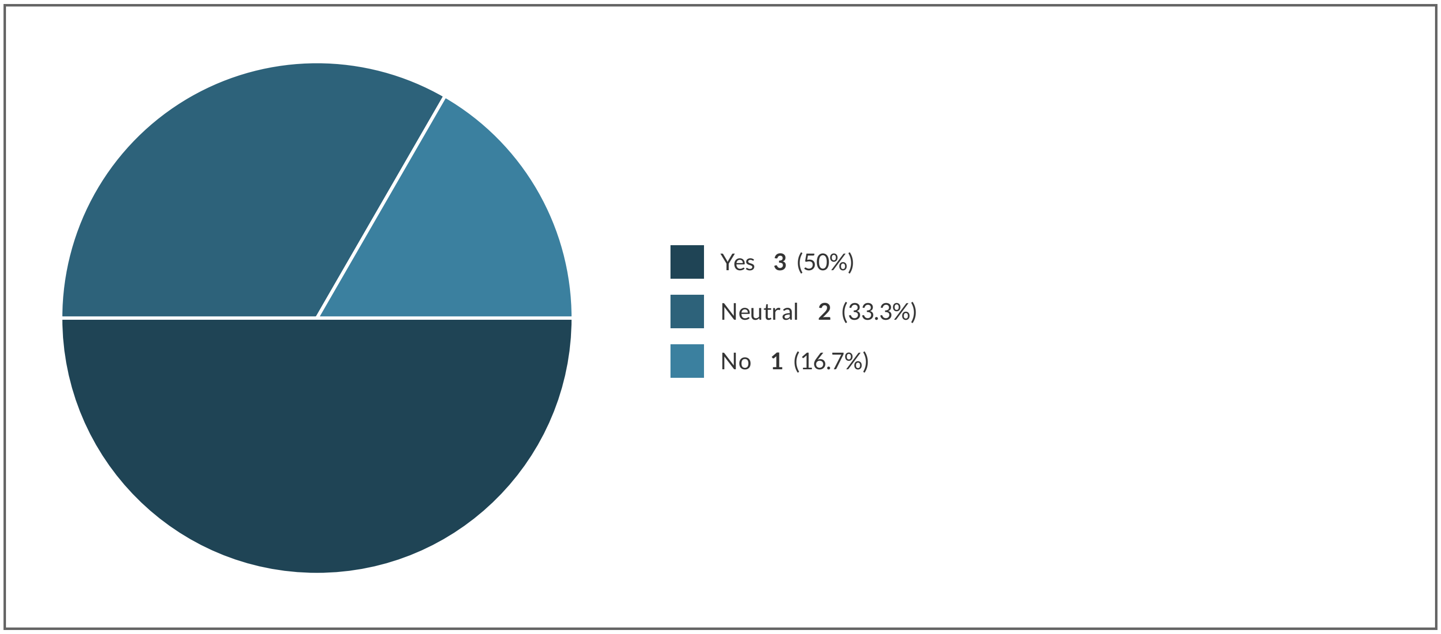
11.5.a Increases the organization's computing power needed - Severity of Cost



11.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



11.a Do you approve of this advice?



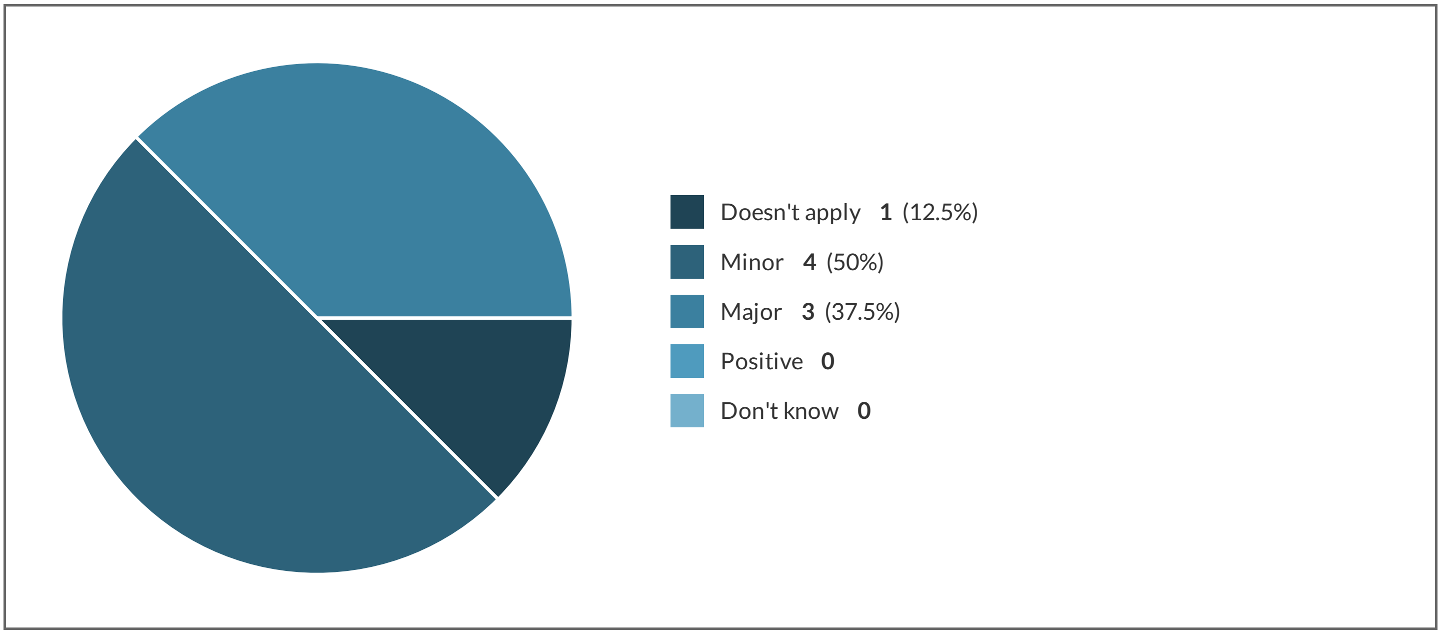
11.b Comments

Showing all 4 responses	
not sure how to answer this!	634211-634202-66098698
Not clear what this means	634211-634202-66532254
I don't understand this question	634211-634202-66532992
Updates are key to a secure business	634211-634202-66754804

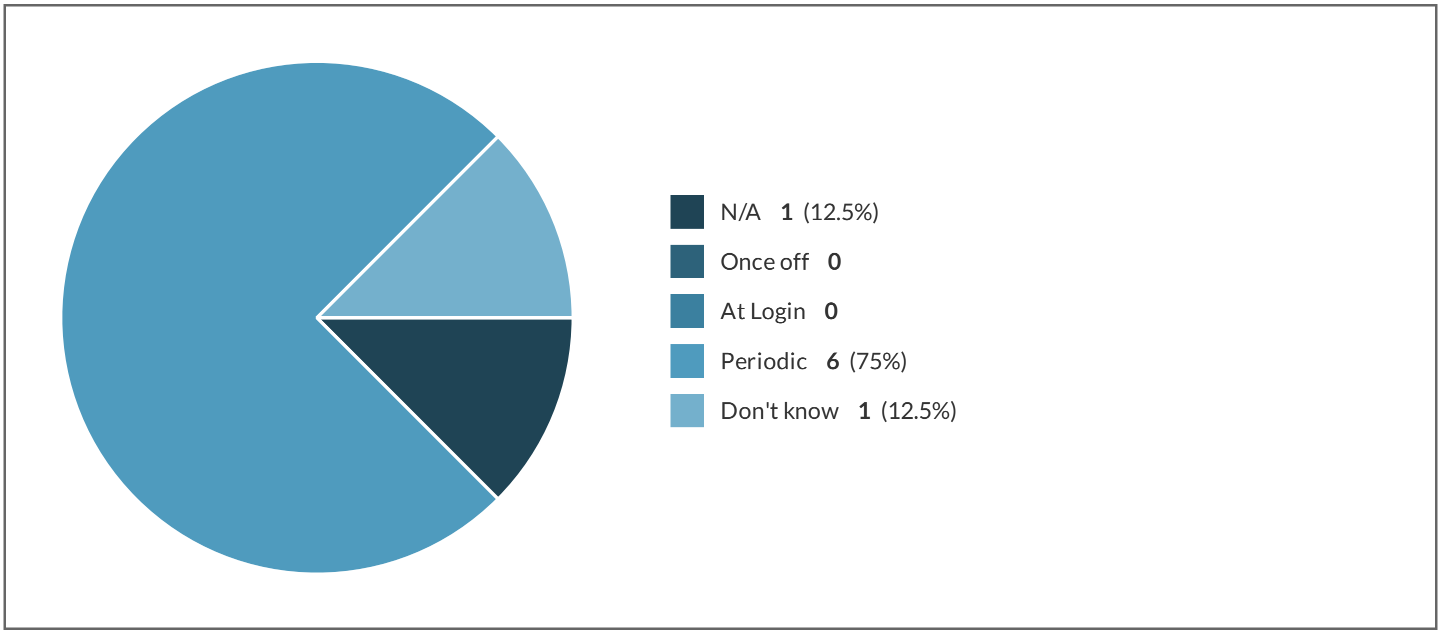
12 A user's software should be kept up to date

12.1 Increased help desk/user support time

12.1.a Increased help desk/user support time - Severity of Cost

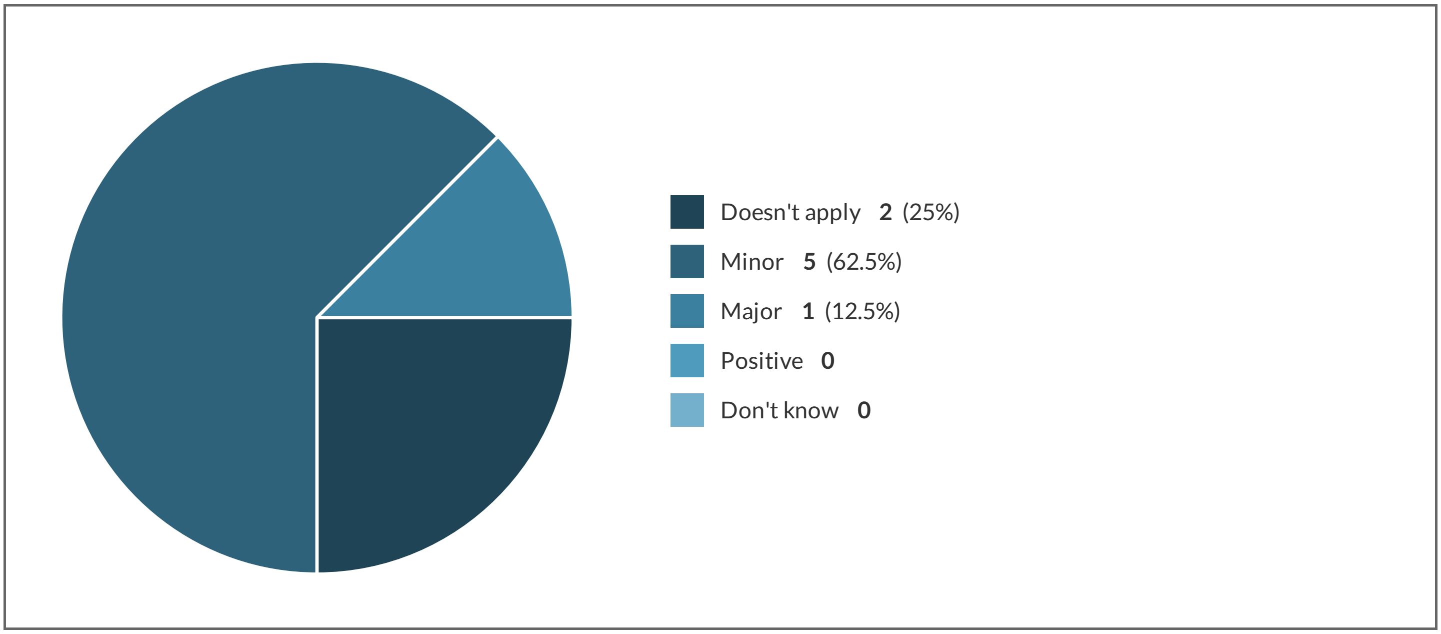


12.1.b Increased help desk/user support time - Frequency Cost is Experienced

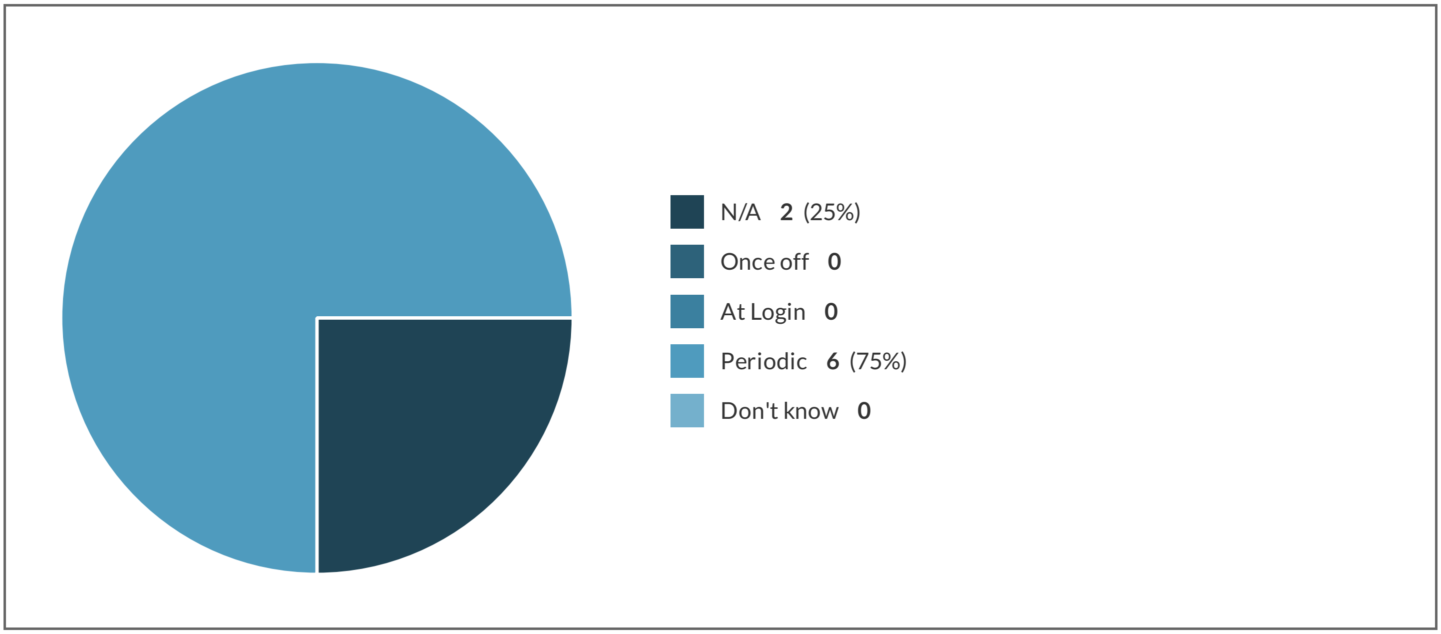


12.2 User education required

12.2.a User education required - Severity of Cost

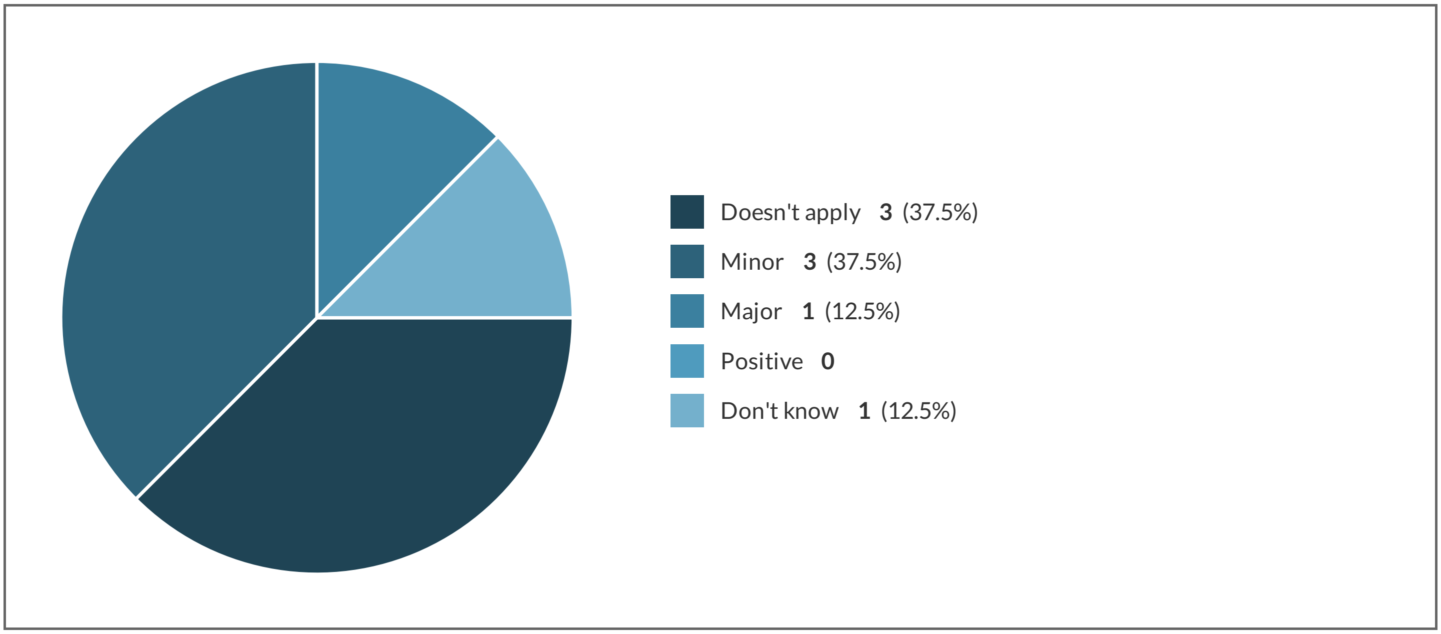


12.2.b User education required - Frequency Cost is Experienced

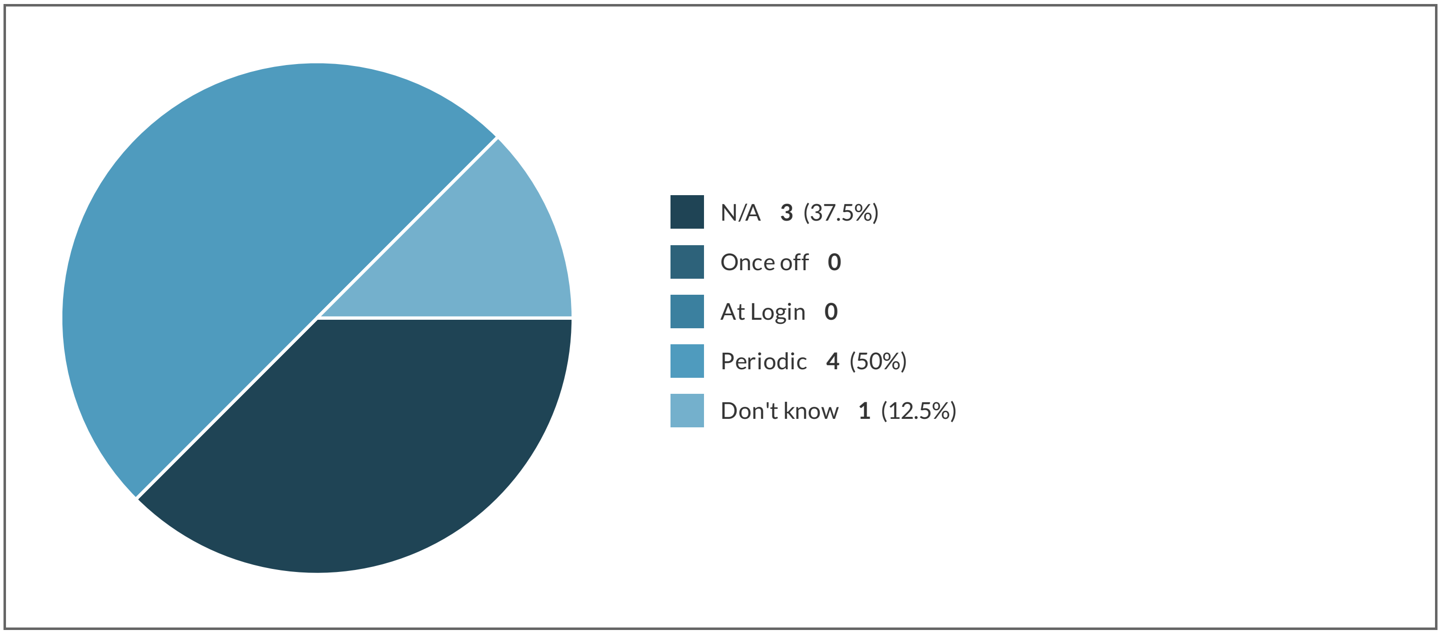


12.3 Organization needs extra resources

12.3.a Organization needs extra resources - Severity of Cost

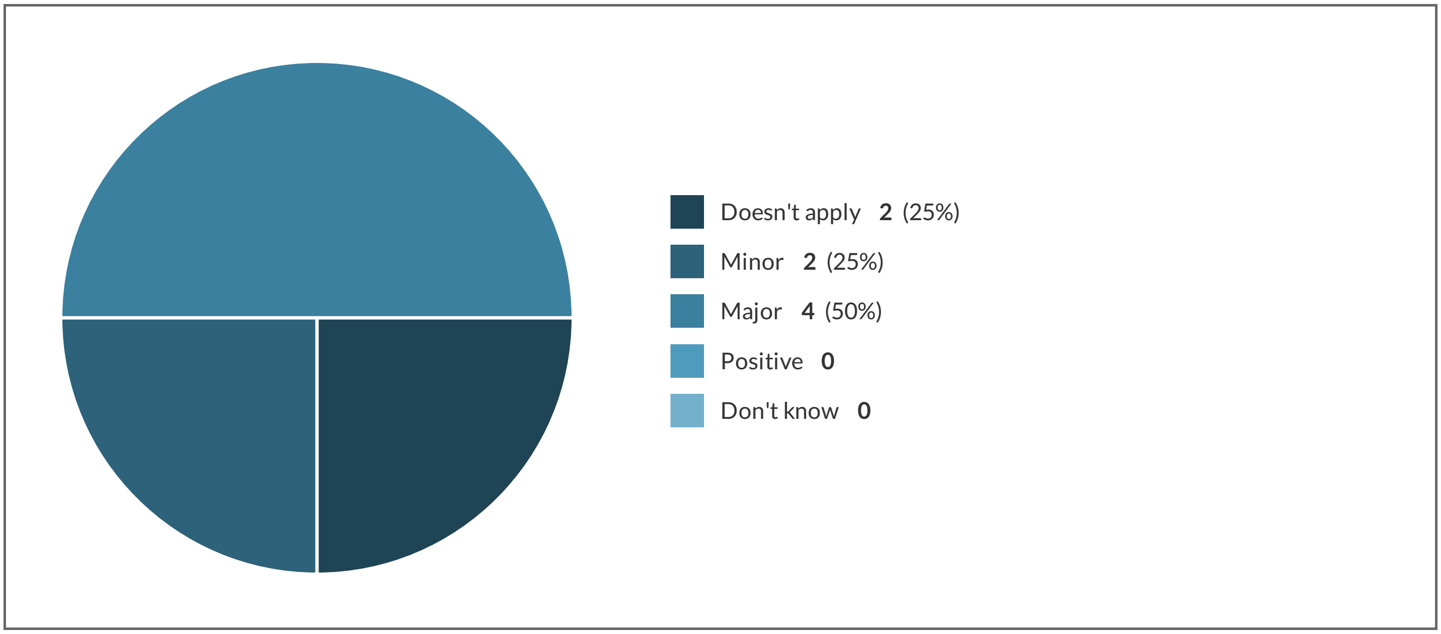


12.3.b Organization needs extra resources - Frequency Cost is Experienced

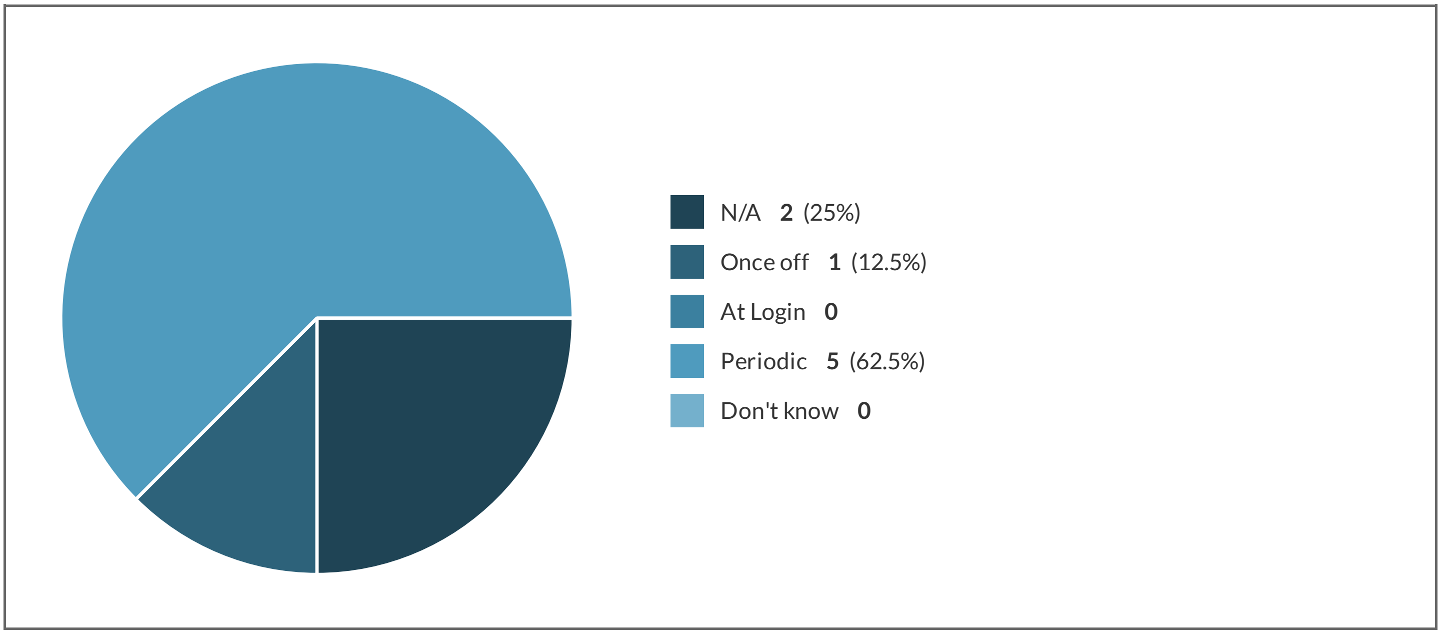


12.4 Takes organization time to implement

12.4.a Takes organization time to implement - Severity of Cost

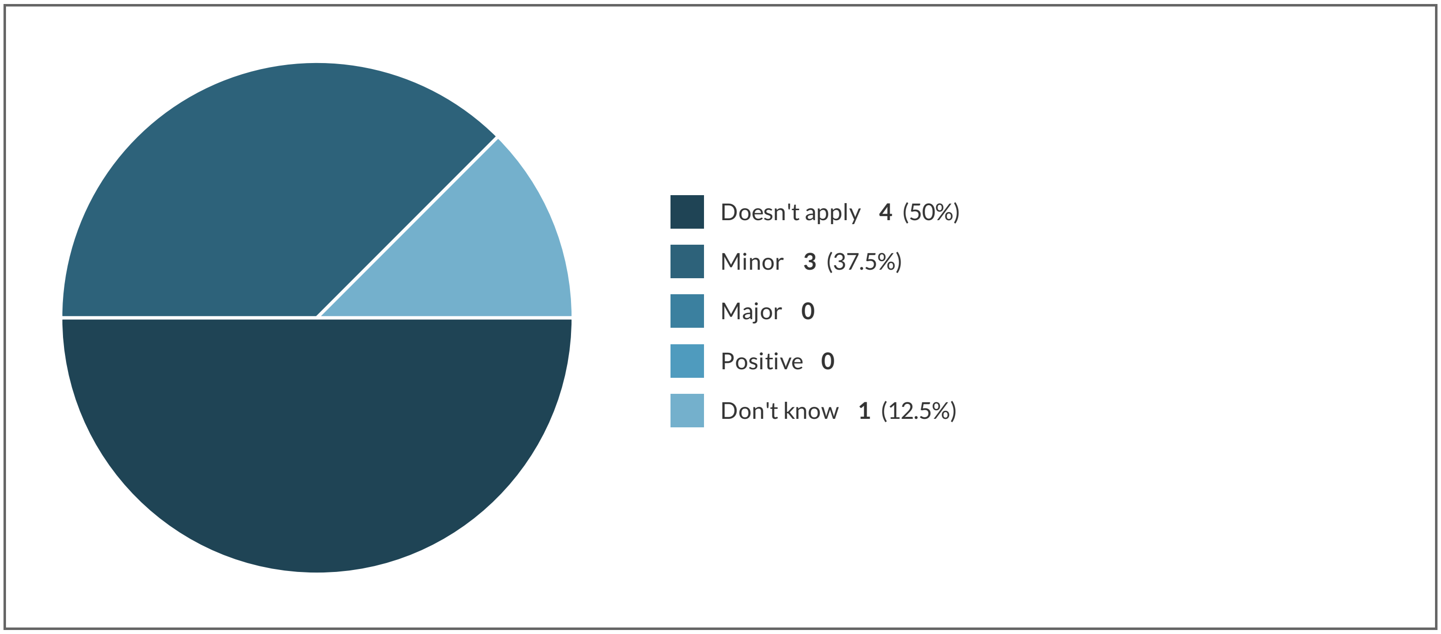


12.4.b Takes organization time to implement - Frequency Cost is Experienced

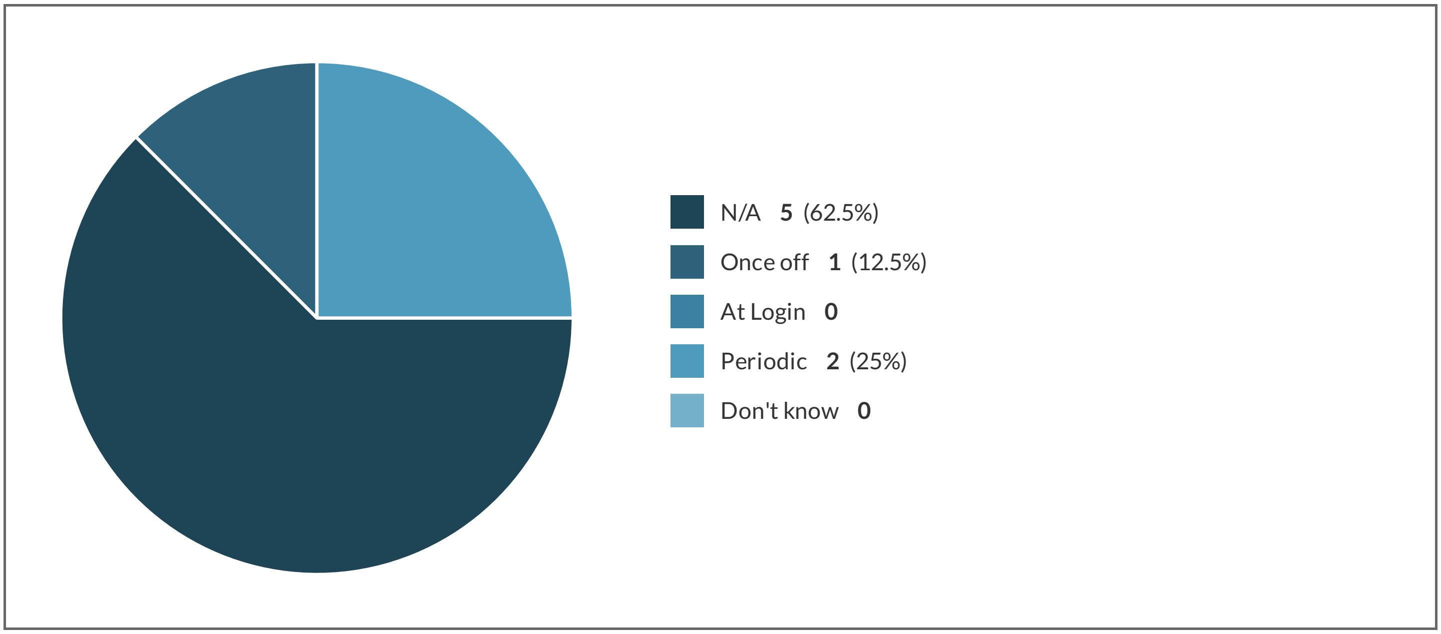


12.5 Increases the organization's computing power needed

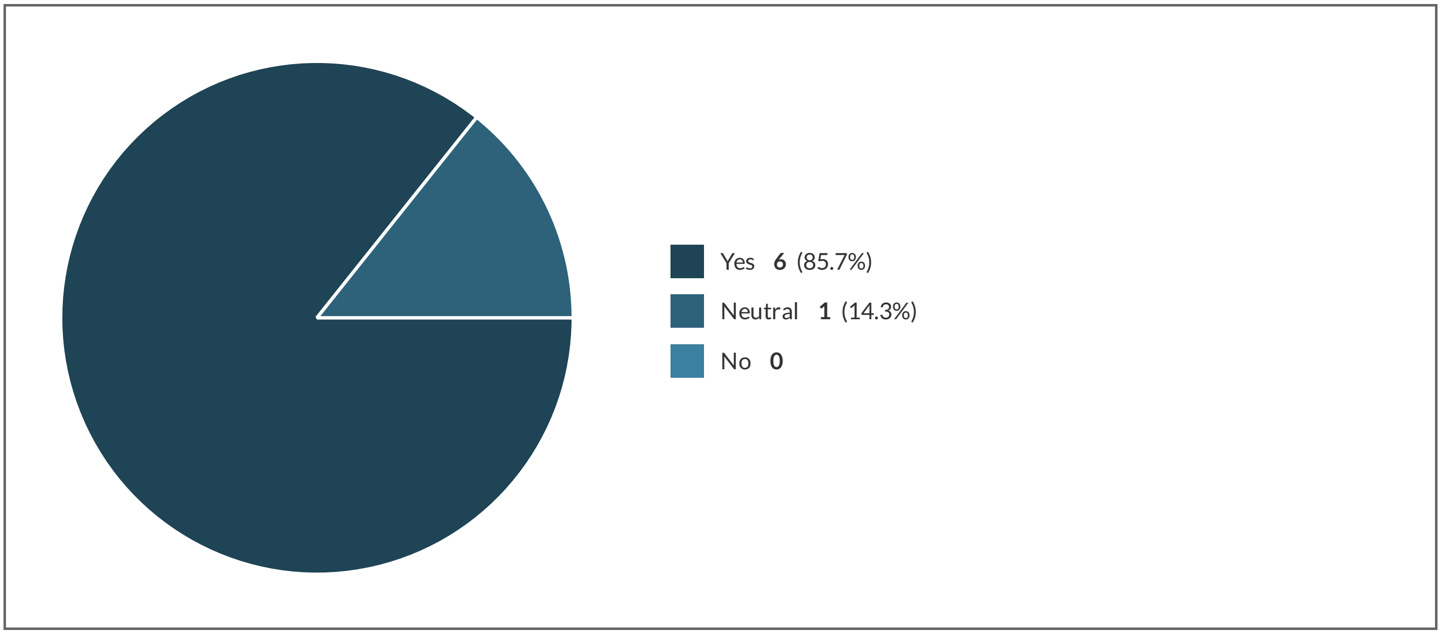
12.5.a Increases the organization's computing power needed - Severity of Cost



12.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



12.a Do you approve of this advice?



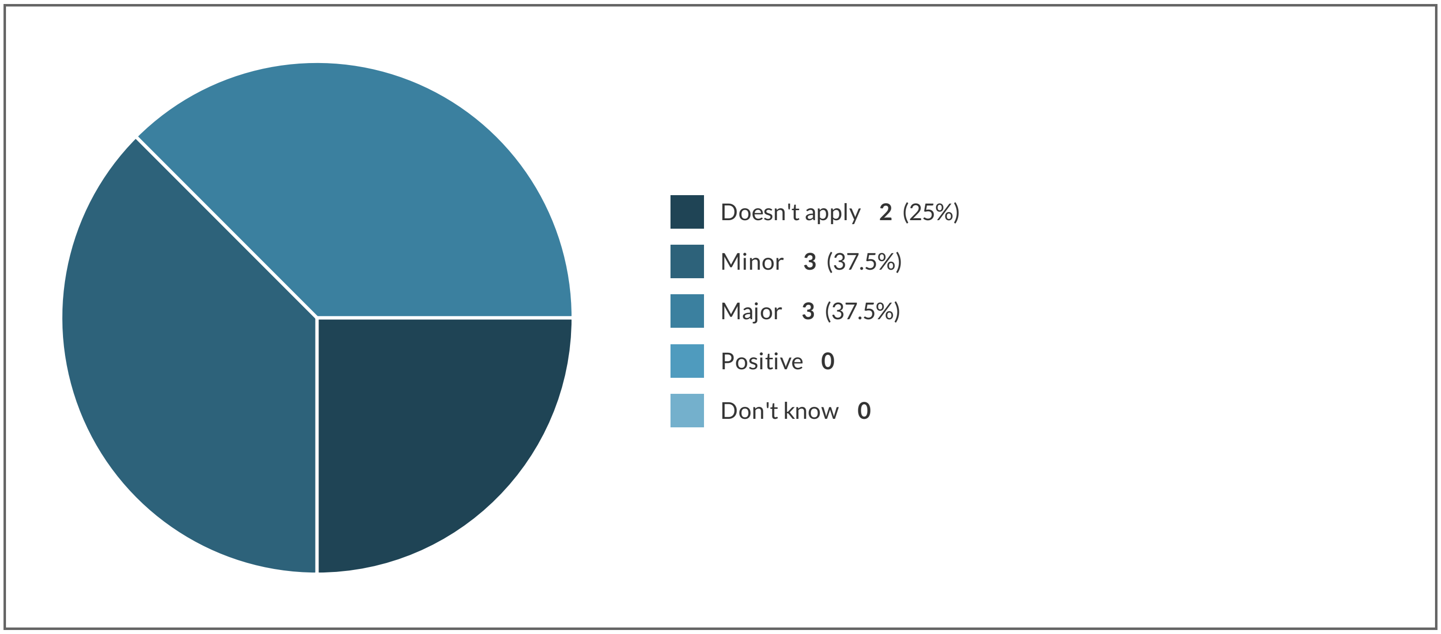
12.b Comments

Showing all 5 responses	
SSCM or equiv	634211-634202-66090277
security updates yes.. other patches depends on use and effects	634211-634202-66098698
needs money and time - dunno if these count as “resources”	634211-634202-66532254
Software needs to ensure its updated and secure across all areas of company's	634211-634202-66754804
I have worked for a large (over 100 million users) company who had their entire internal network compromised by employees using out of date VPN software	634211-634202-66754952

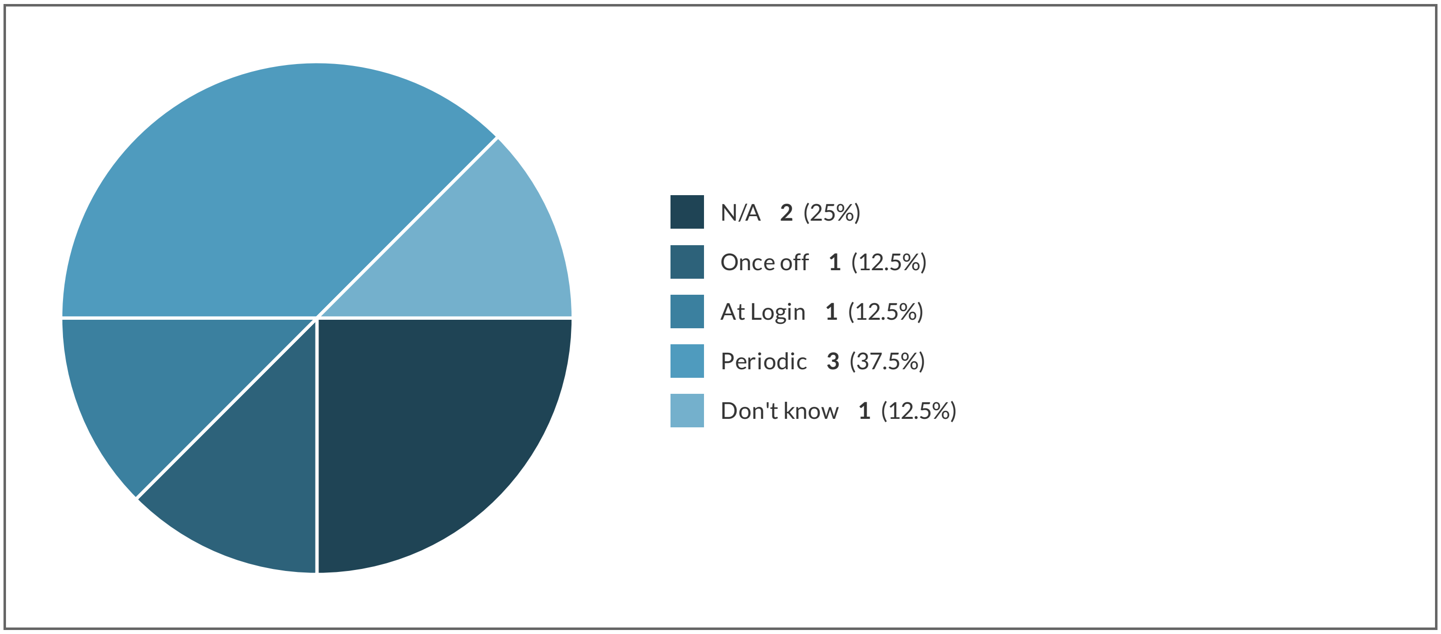
13 Users should have to use some form of 2-factor authentication

13.1 Increased help desk/user support time

13.1.a Increased help desk/user support time - Severity of Cost

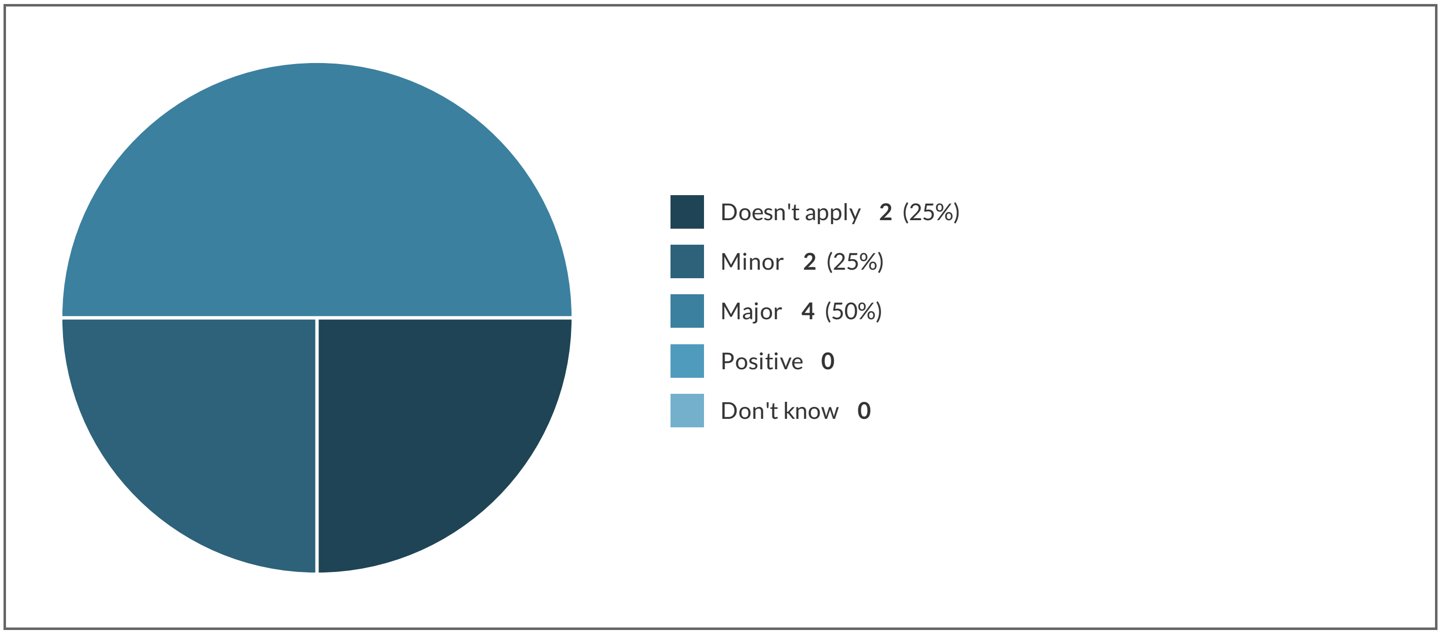


13.1.b Increased help desk/user support time - Frequency Cost is Experienced

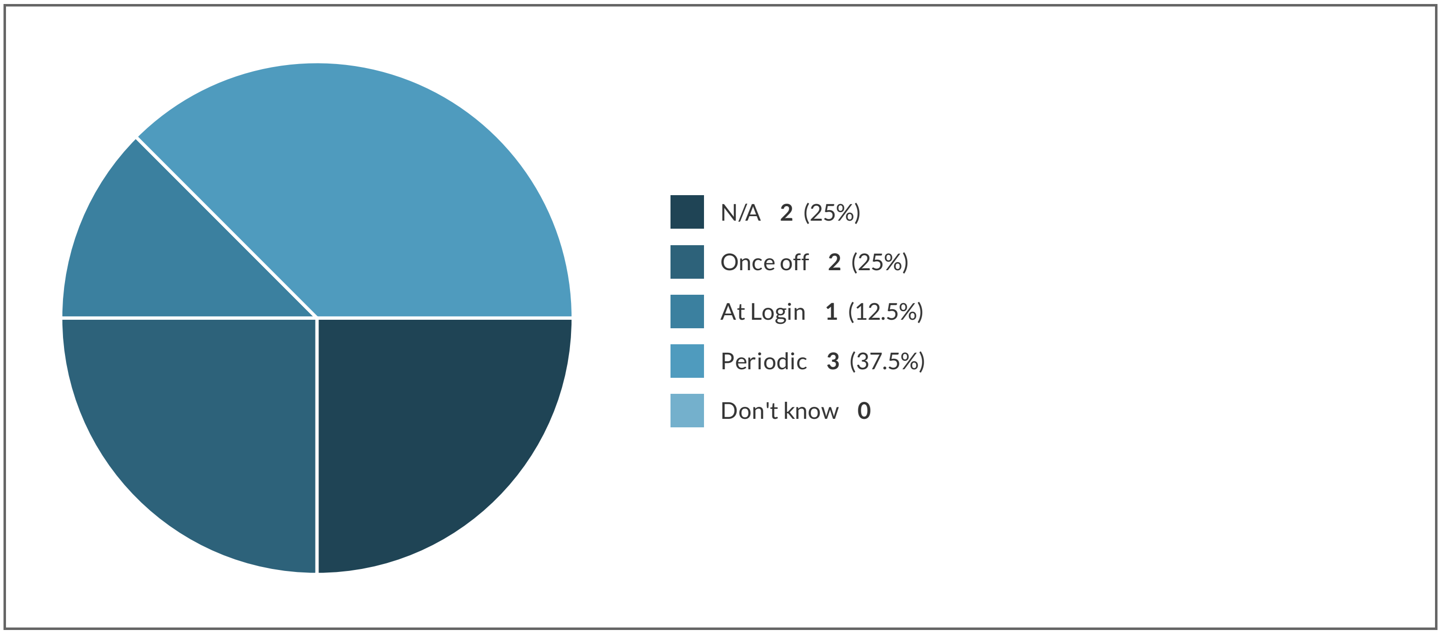


13.2 User education required

13.2.a User education required - Severity of Cost

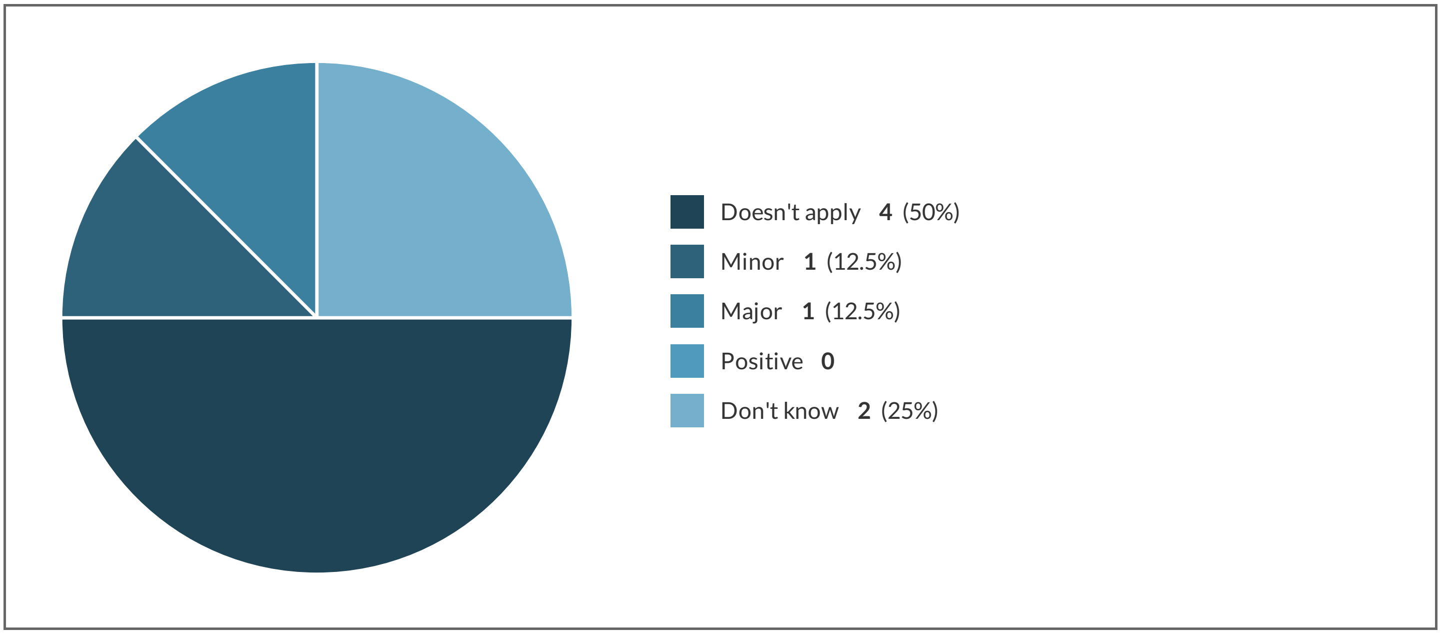


13.2.b User education required - Frequency Cost is Experienced

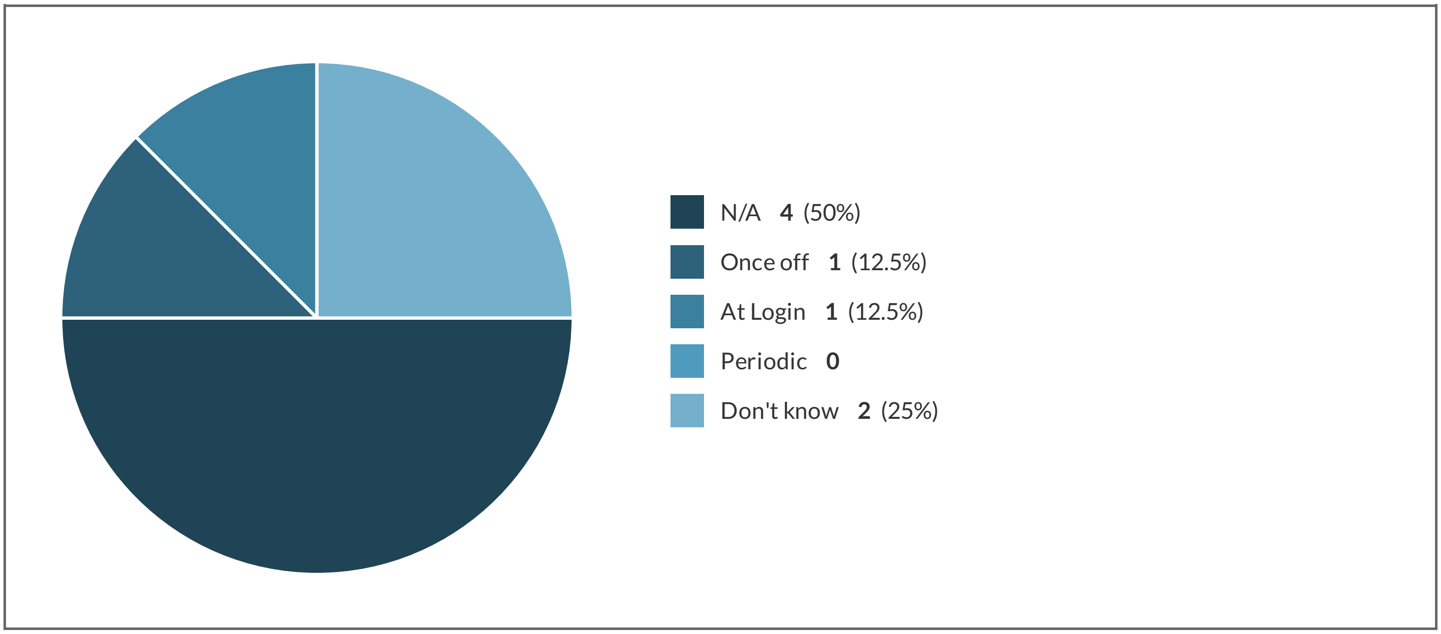


13.3 Organization needs extra resources

13.3.a Organization needs extra resources - Severity of Cost

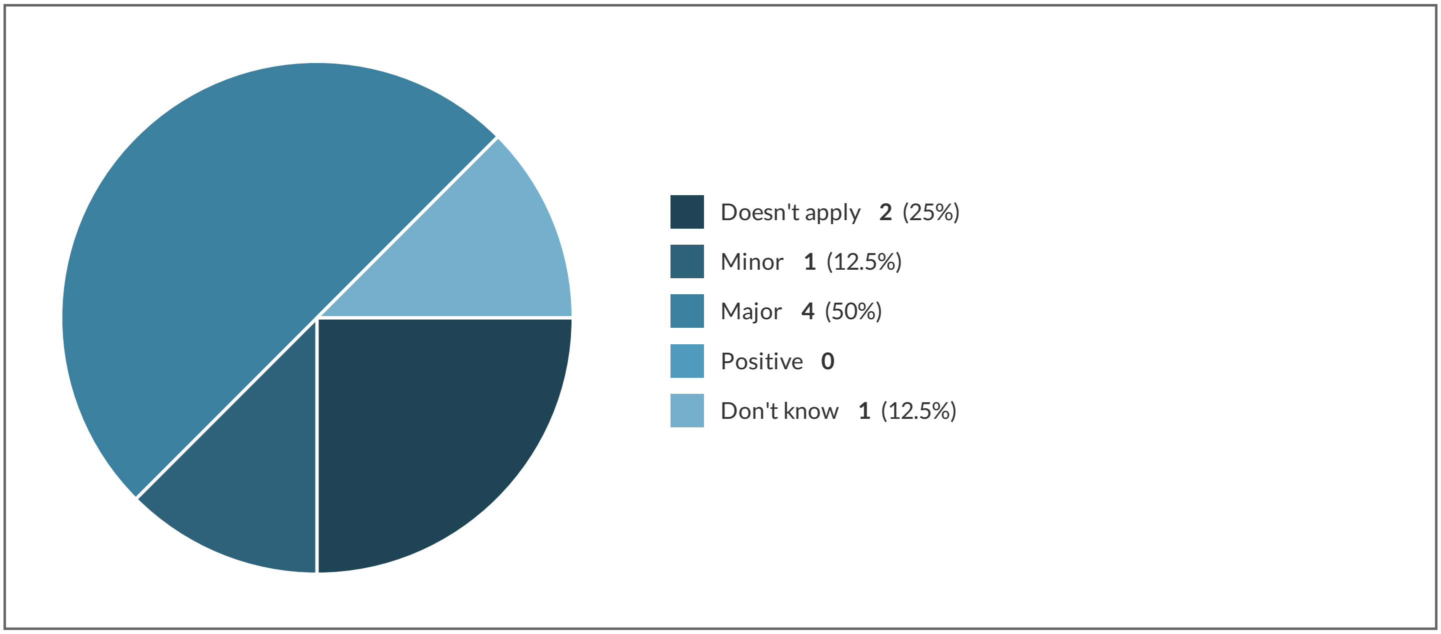


13.3.b Organization needs extra resources - Frequency Cost is Experienced

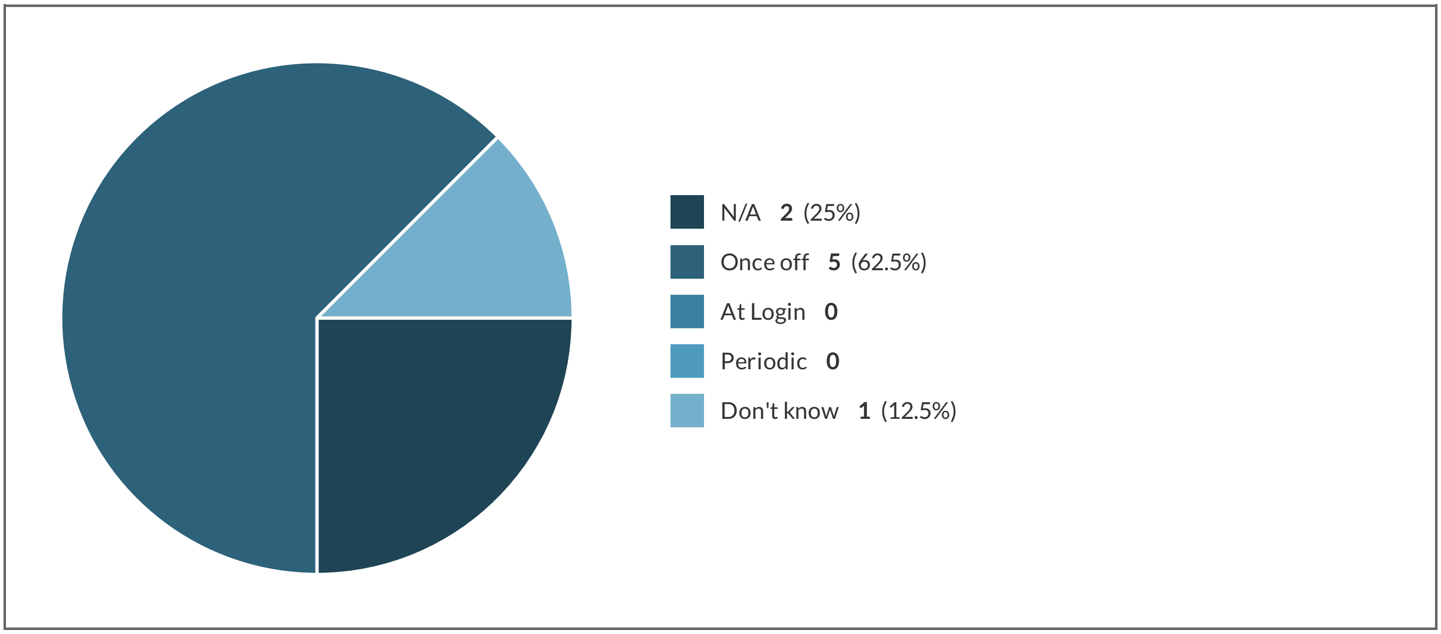


13.4 Takes organization time to implement

13.4.a Takes organization time to implement - Severity of Cost

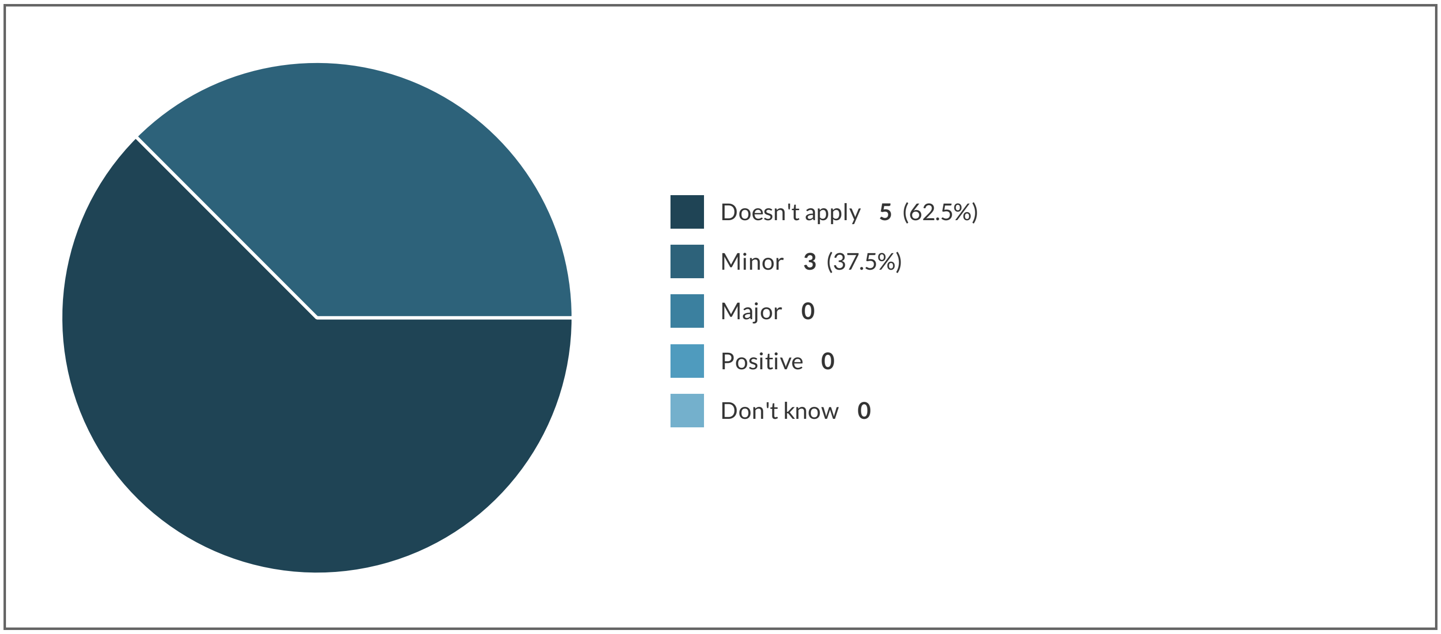


13.4.b Takes organization time to implement - Frequency Cost is Experienced

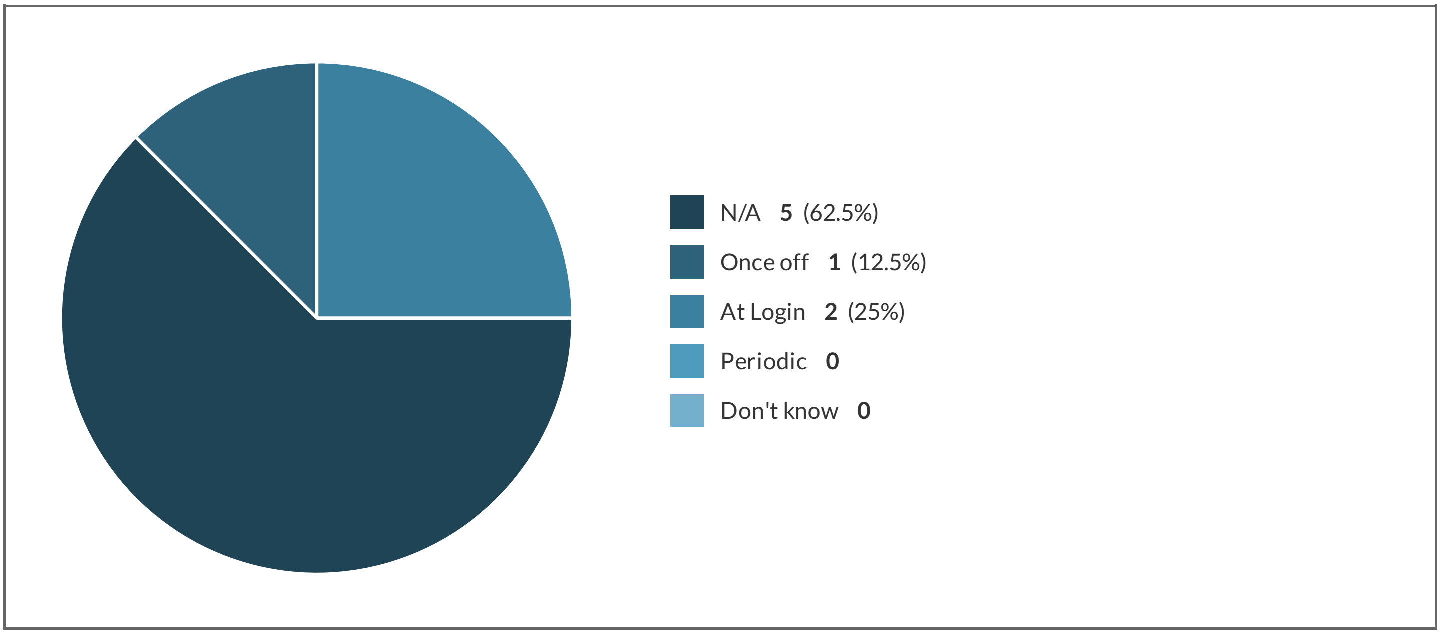


13.5 Increases the organization's computing power needed

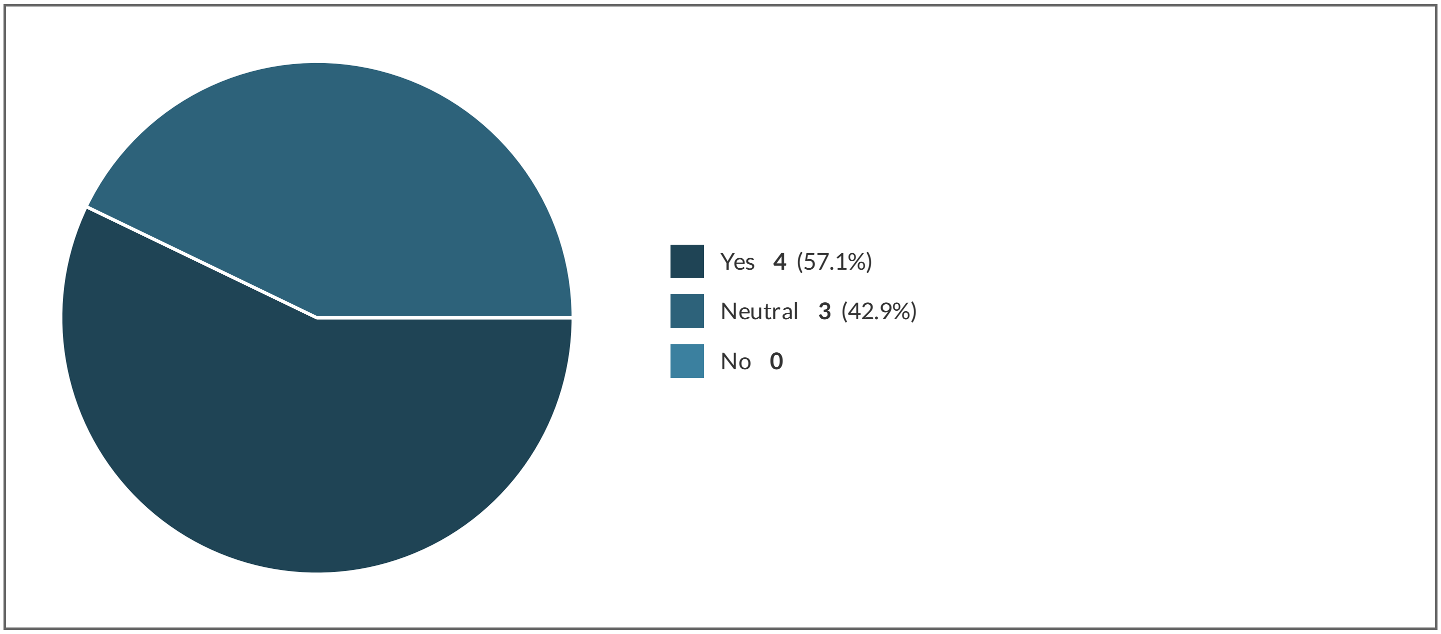
13.5.a Increases the organization's computing power needed - Severity of Cost



13.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



13.a Do you approve of this advice?



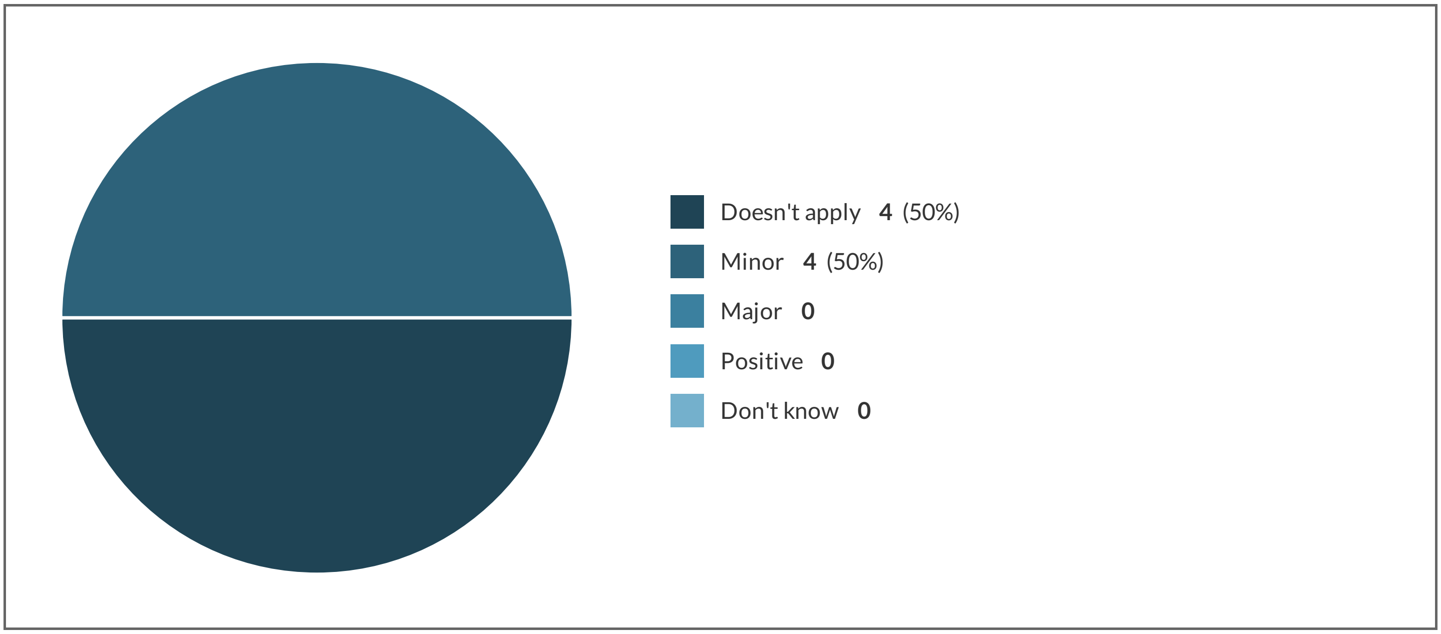
13.b Comments

Showing all 4 responses	
2FA is sector dependent	634211-634202-66090277
2FA should be common place across company's but unfortunately it's not	634211-634202-66754804
Should be completely mandatory. Be it a push notification to their phone or some randomly generated OTP or both. Some form of MFA should be used.	634211-634202-66754952
Costs can be variable depending on implimentation, danger of requiring users to turn over more personal data to third parties such as Google. Costs impacted when using hardware 2FA devices.	634211-634202-66871889

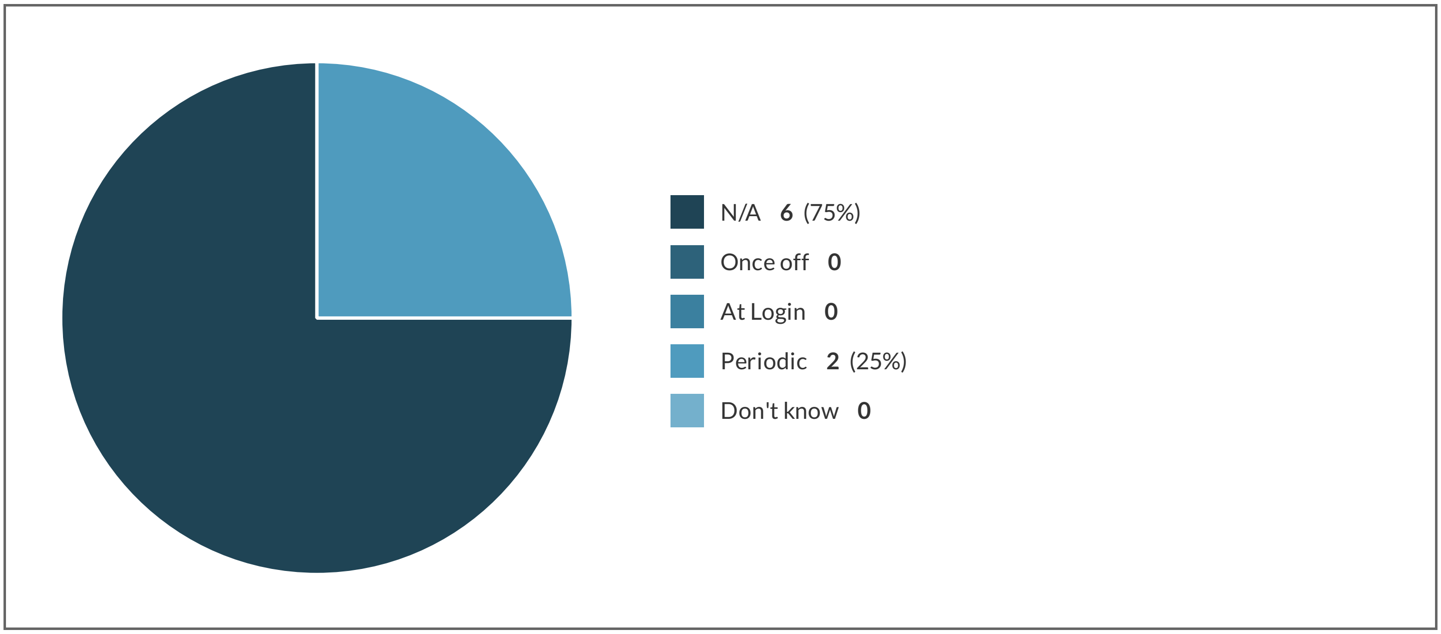
14 If a user is using a password manager, long random passwords should be generated

14.1 Increased help desk/user support time

14.1.a Increased help desk/user support time - Severity of Cost

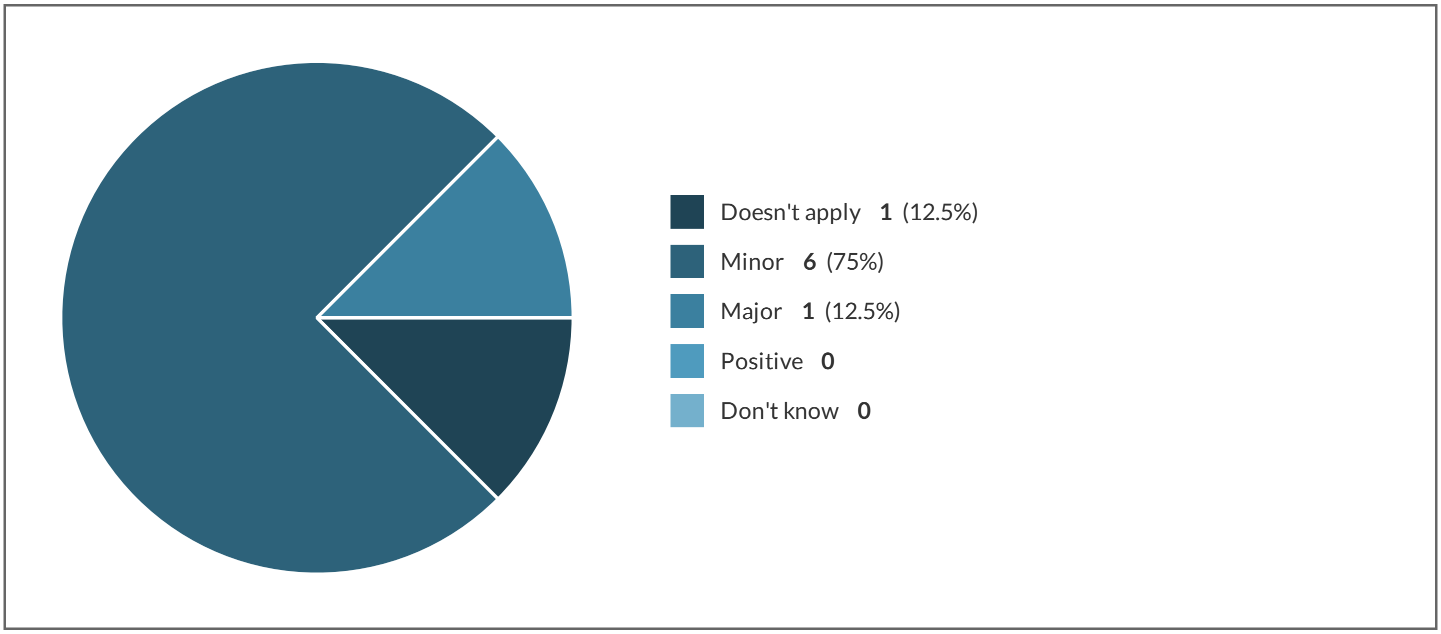


14.1.b Increased help desk/user support time - Frequency Cost is Experienced

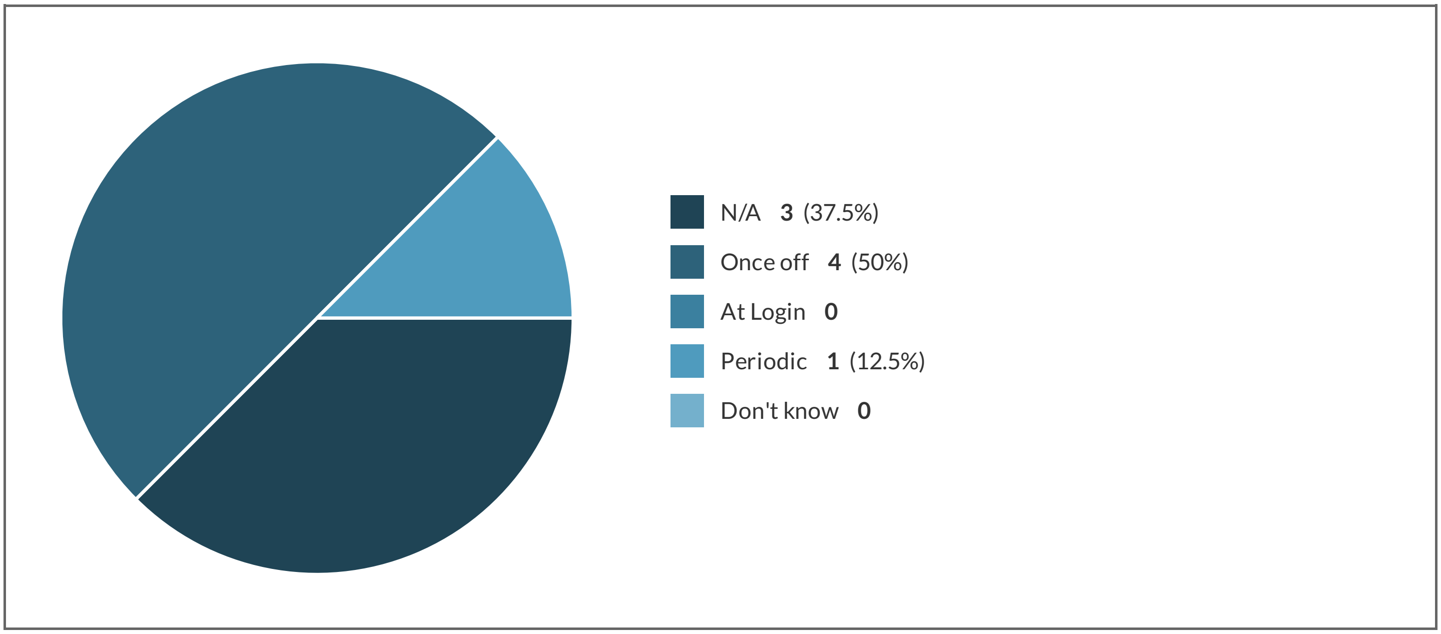


14.2 User education required

14.2.a User education required - Severity of Cost

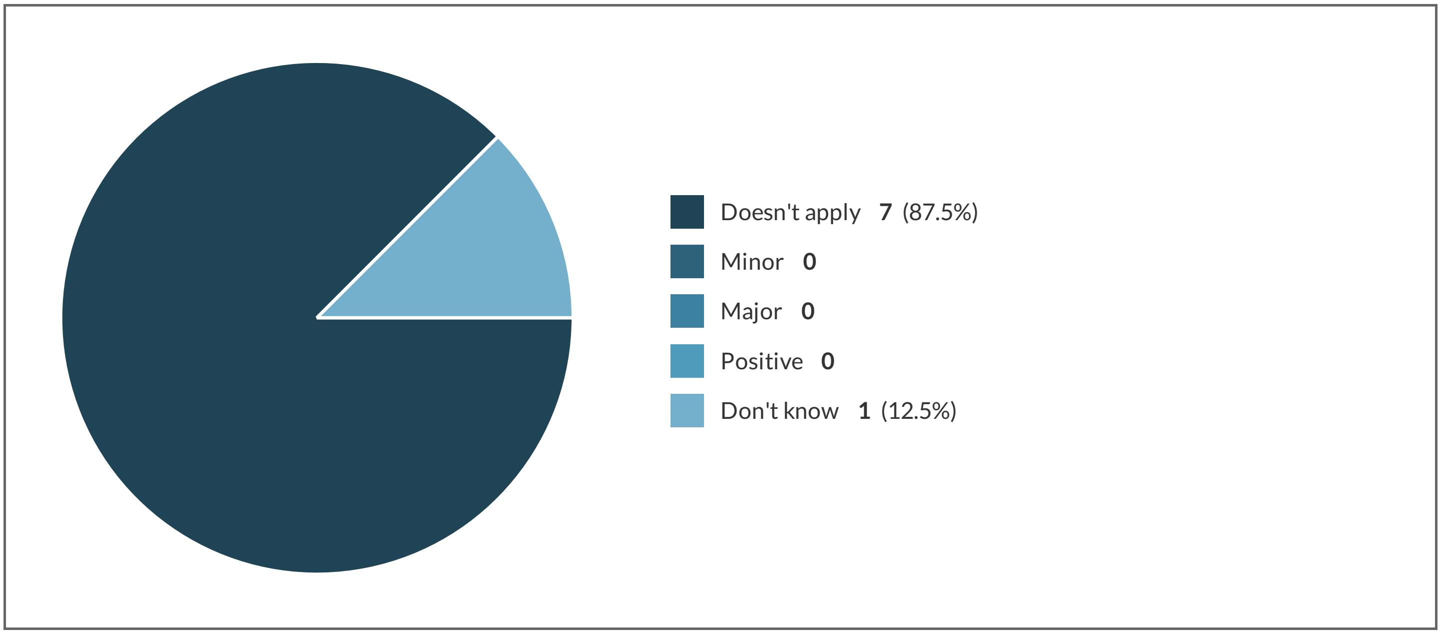


14.2.b User education required - Frequency Cost is Experienced

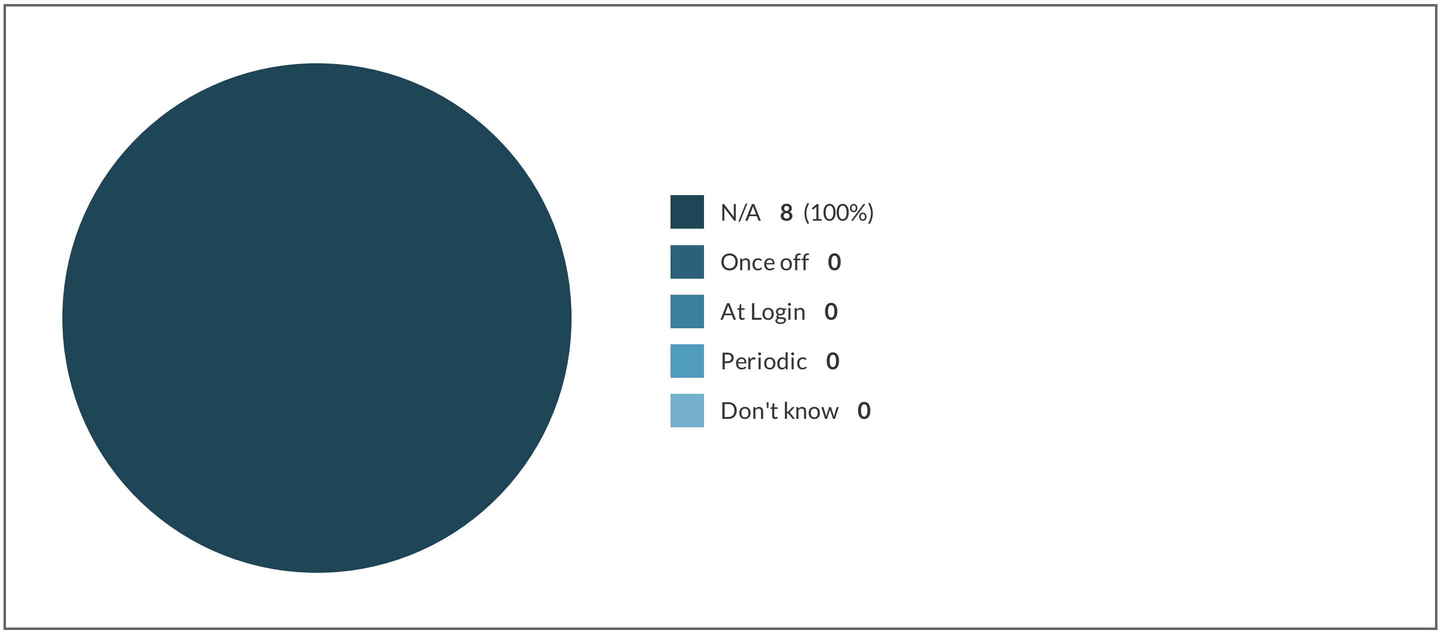


14.3 Organization needs extra resources

14.3.a Organization needs extra resources - Severity of Cost

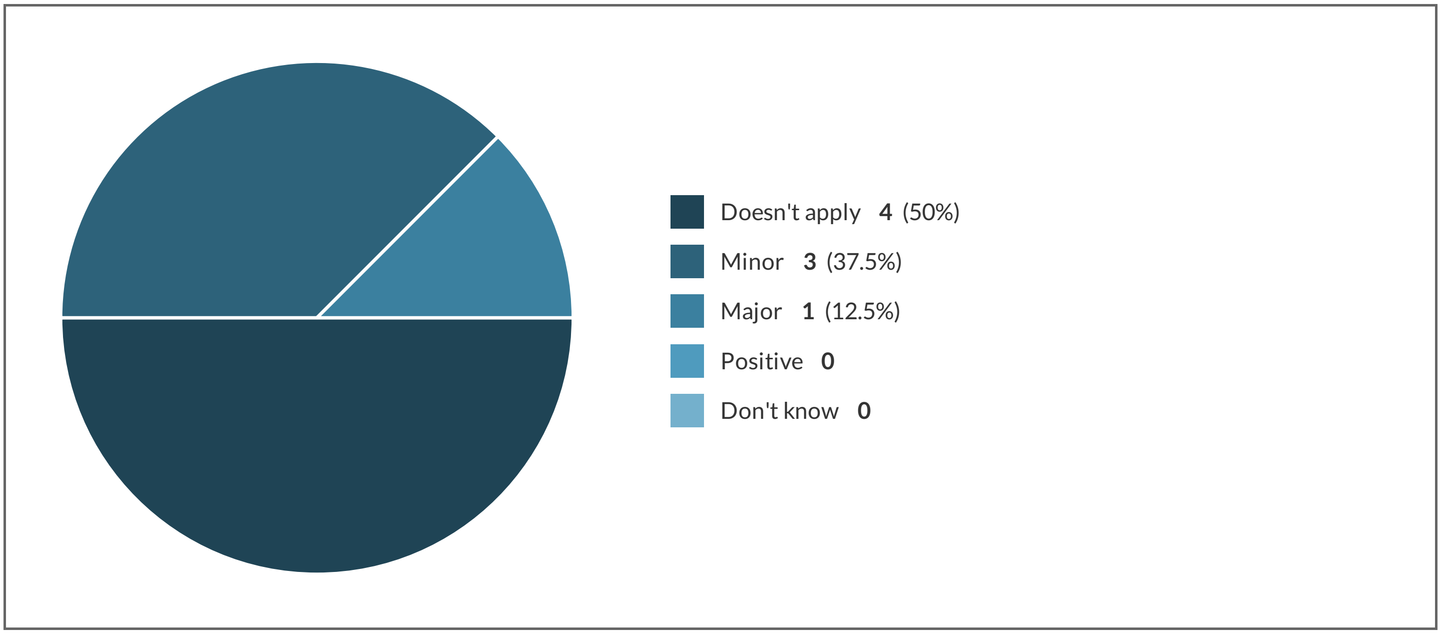


14.3.b Organization needs extra resources - Frequency Cost is Experienced

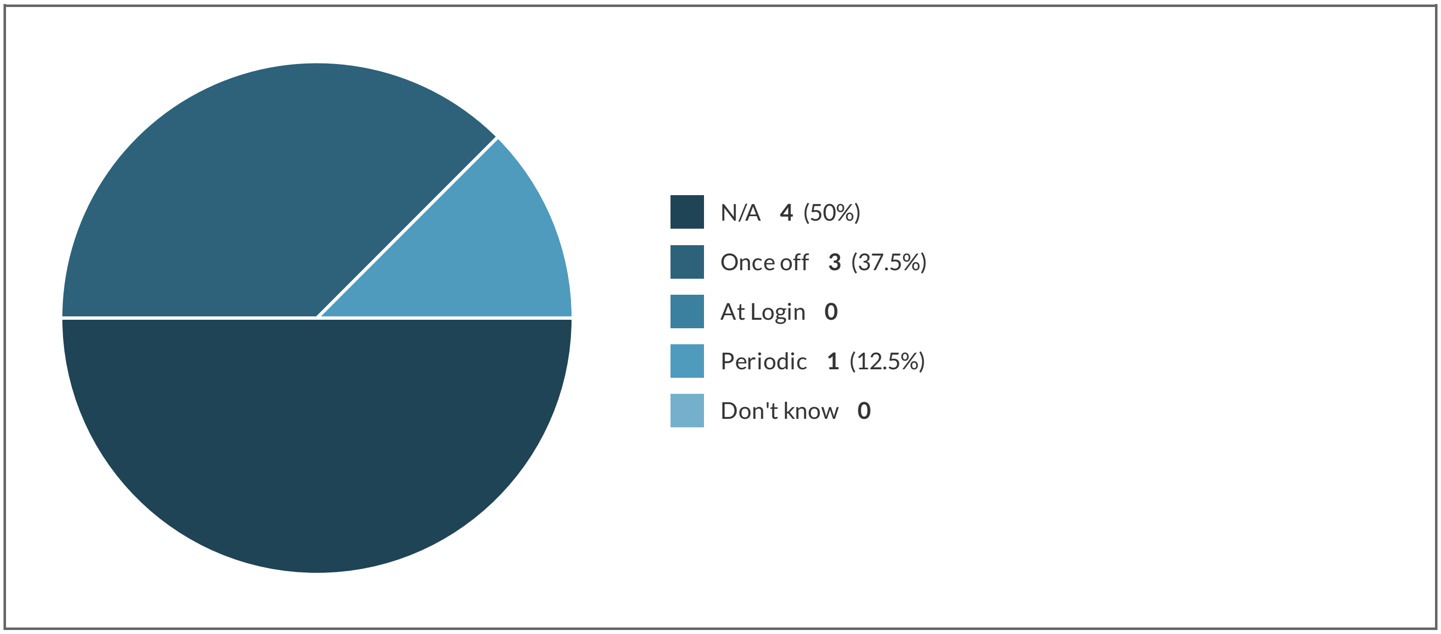


14.4 Takes organization time to implement

14.4.a Takes organization time to implement - Severity of Cost

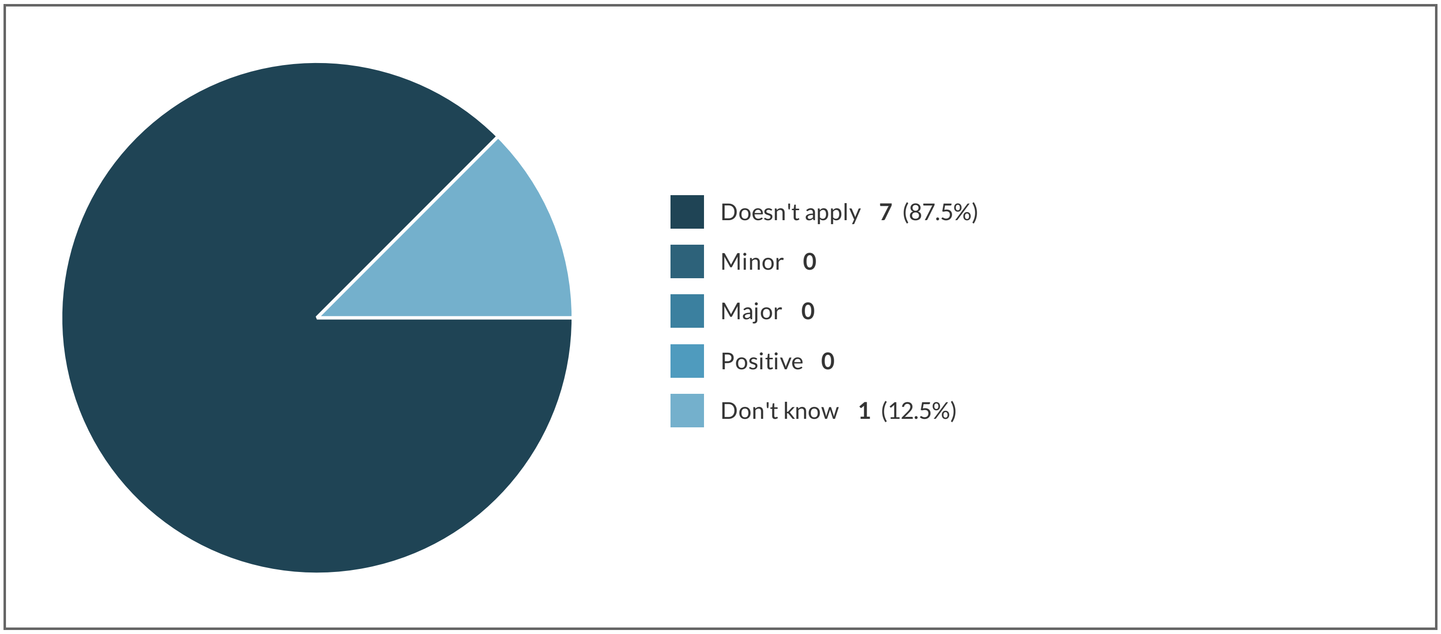


14.4.b Takes organization time to implement - Frequency Cost is Experienced

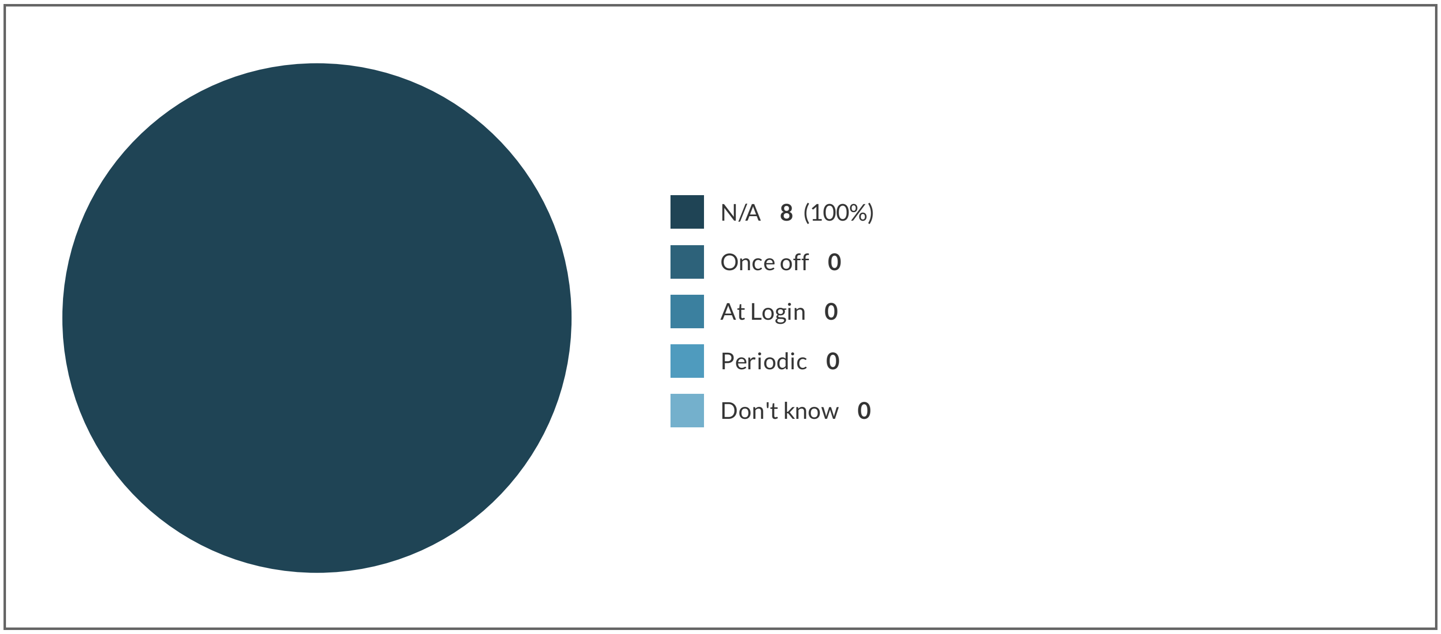


14.5 Increases the organization's computing power needed

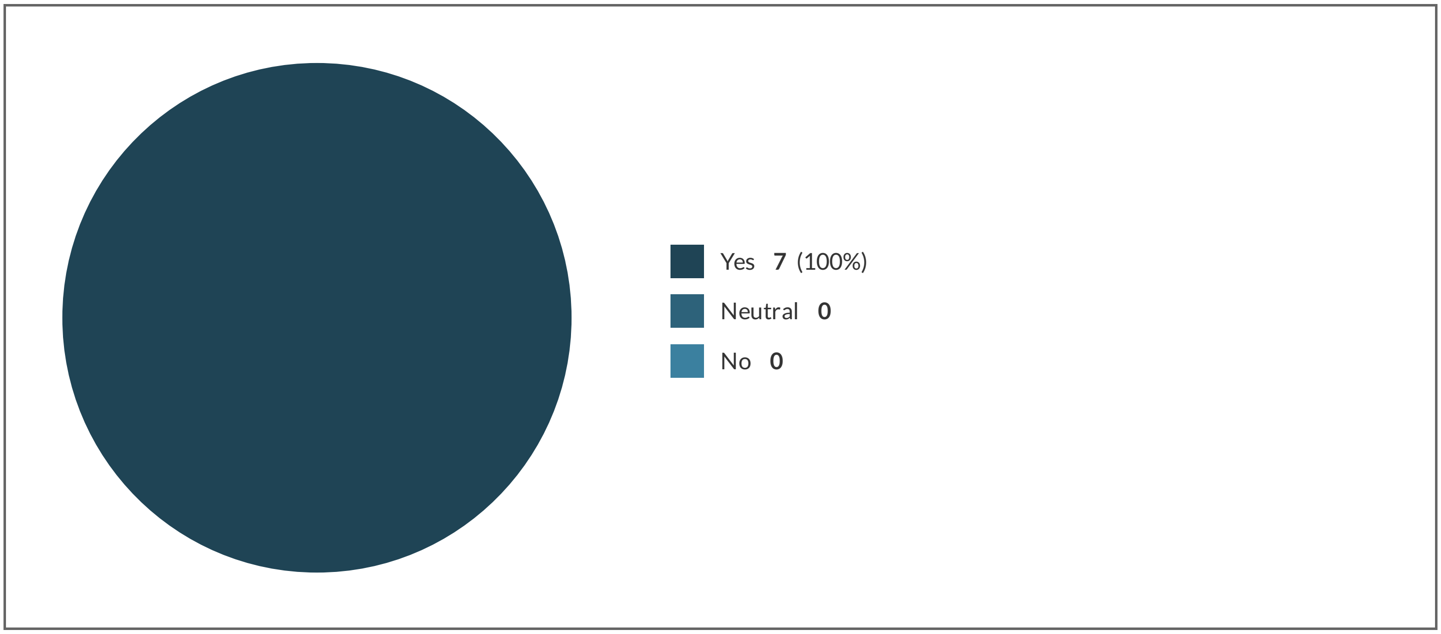
14.5.a Increases the organization's computing power needed - Severity of Cost



14.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



14.a Do you approve of this advice?



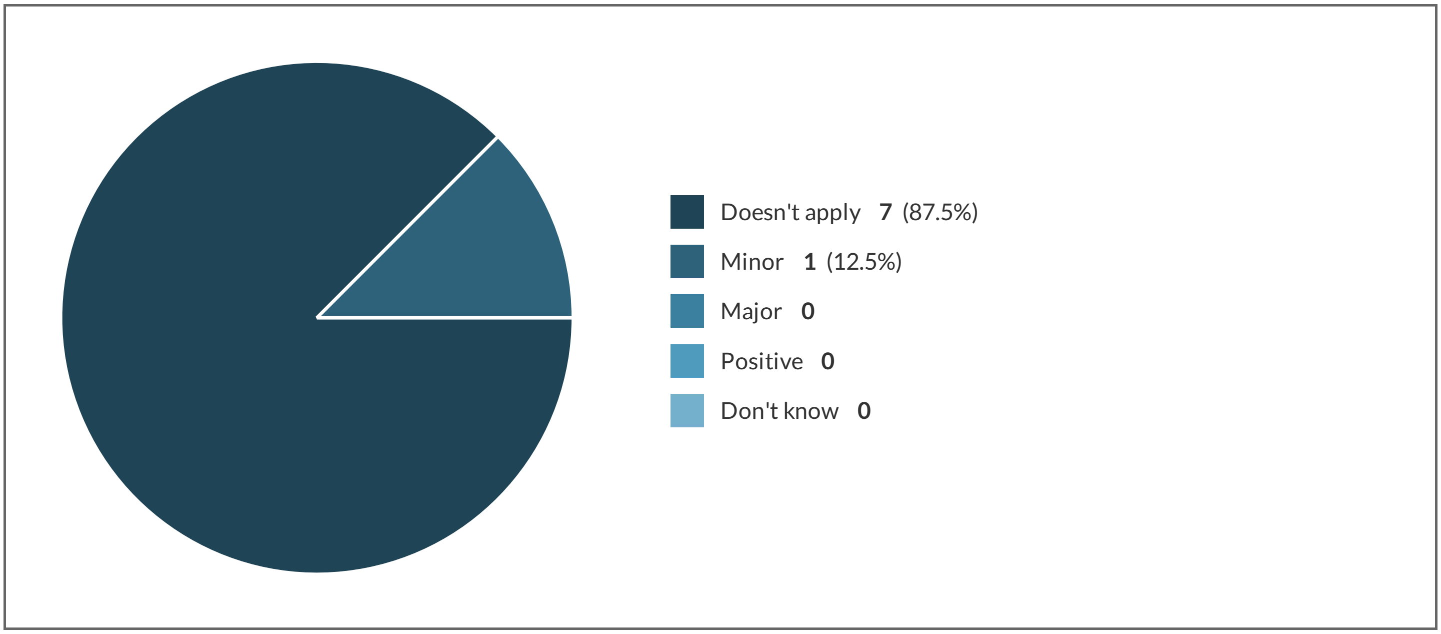
14.b Comments

Showing all 5 responses	
Assumes that the user will always have access to their password manager. SaaS on off site work may limit this.	634211-634202-66090277
some logins tend to have limits on password length and characters used	634211-634202-66098698
If there is use of a password manager then yes all passwords should be as long as they can be	634211-634202-66754804
LastPass has a great enterprise plan that I think any mid-sized company should invest in for their employees	634211-634202-66754952
Costs can depend on software v hardware password managers	634211-634202-66871889

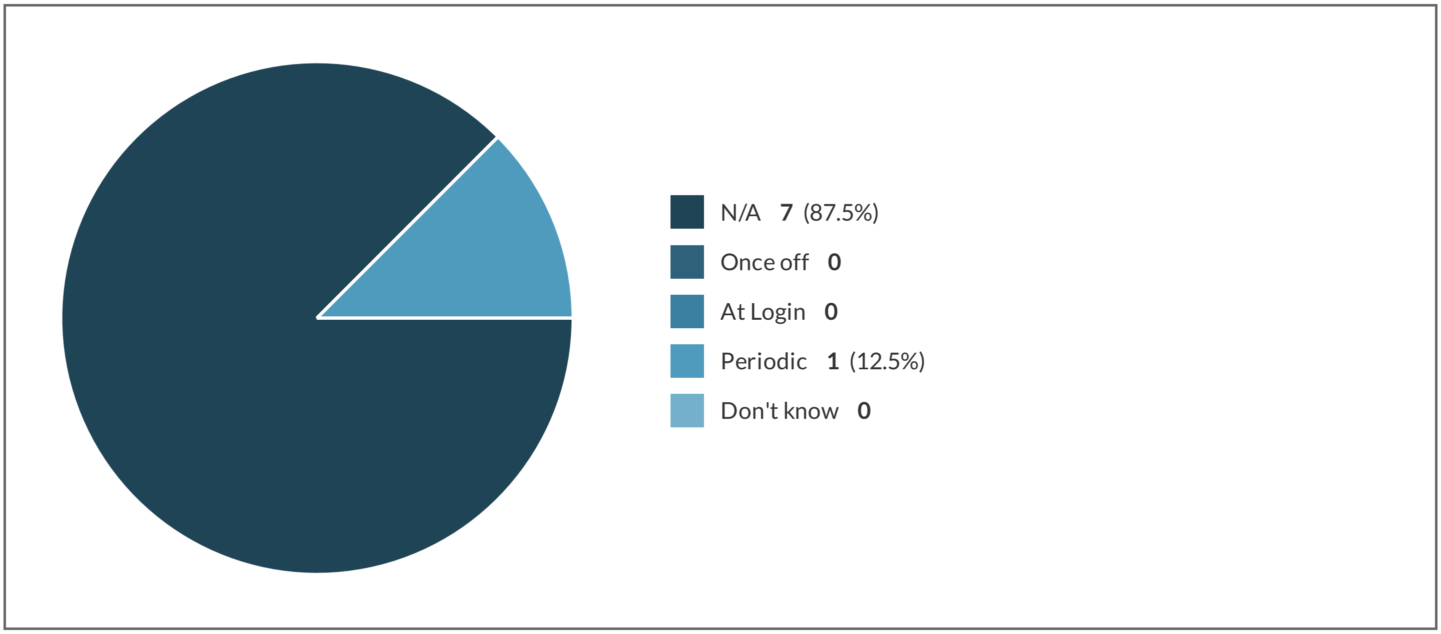
15 If physically distributed, a generated password should be sent in a sealed envelope

15.1 Increased help desk/user support time

15.1.a Increased help desk/user support time - Severity of Cost

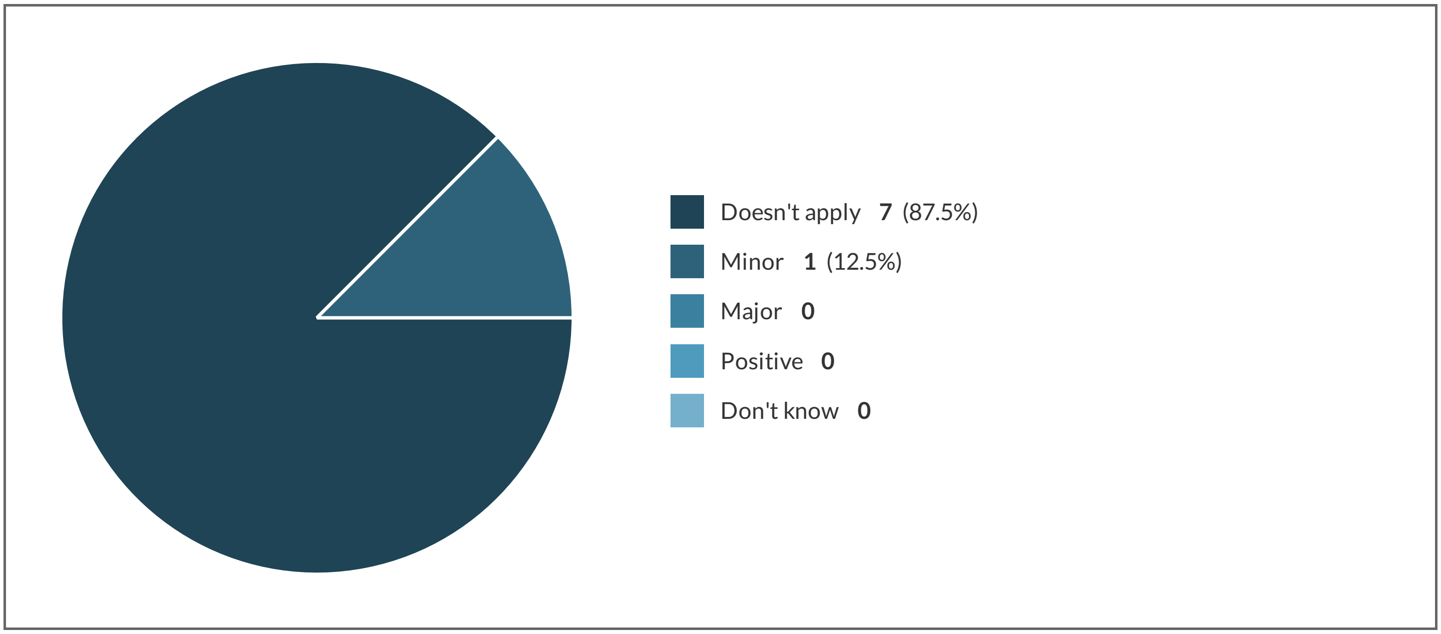


15.1.b Increased help desk/user support time - Frequency Cost is Experienced

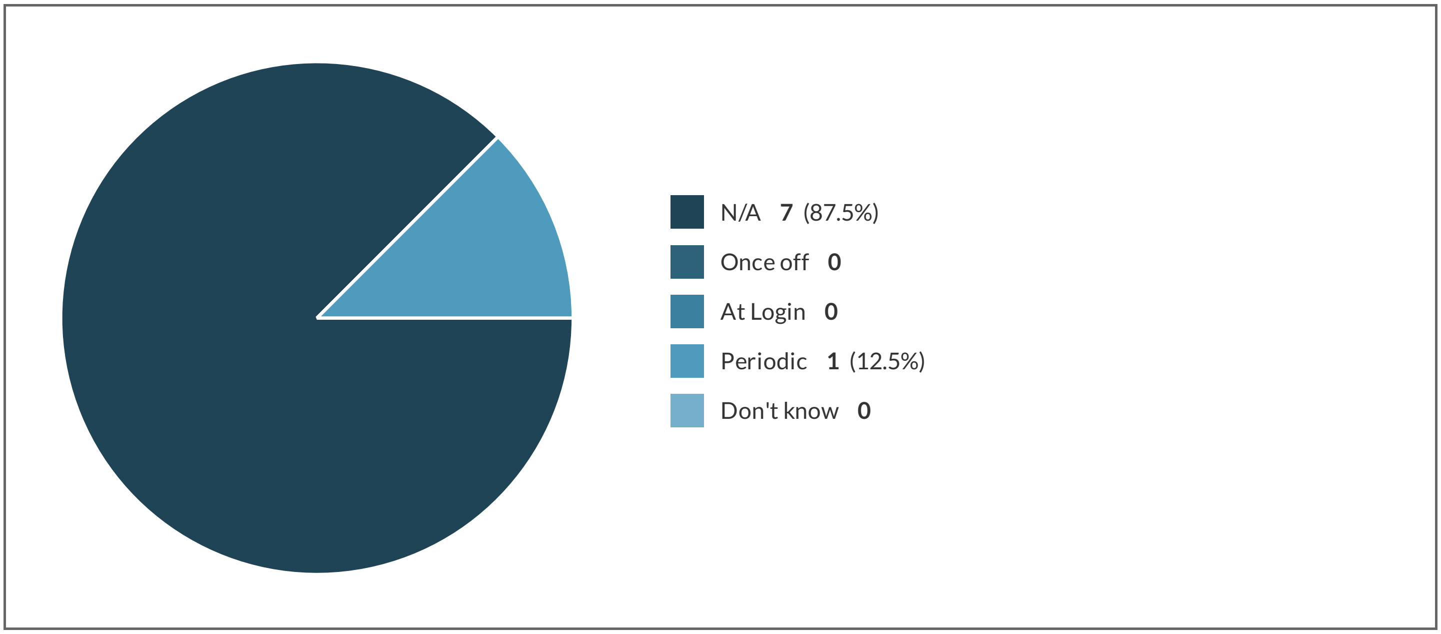


15.2 User education required

15.2.a User education required - Severity of Cost

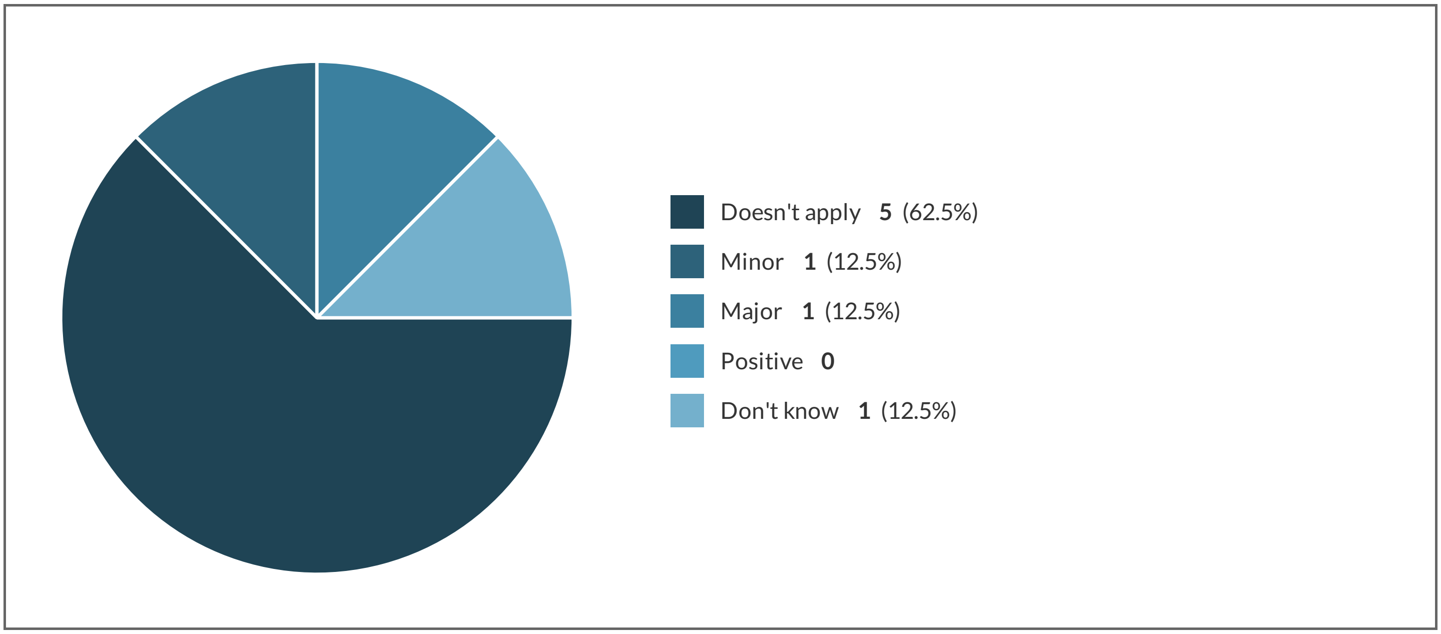


15.2.b User education required - Frequency Cost is Experienced

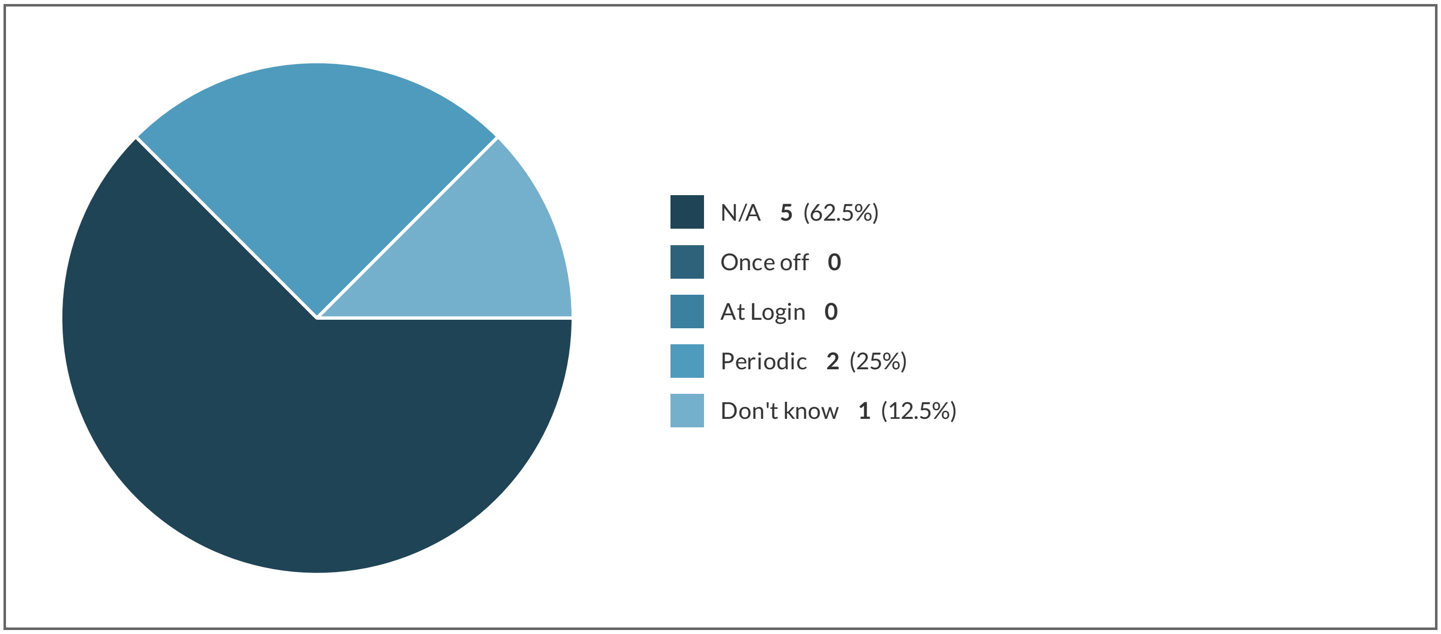


15.3 Organization needs extra resources

15.3.a Organization needs extra resources - Severity of Cost

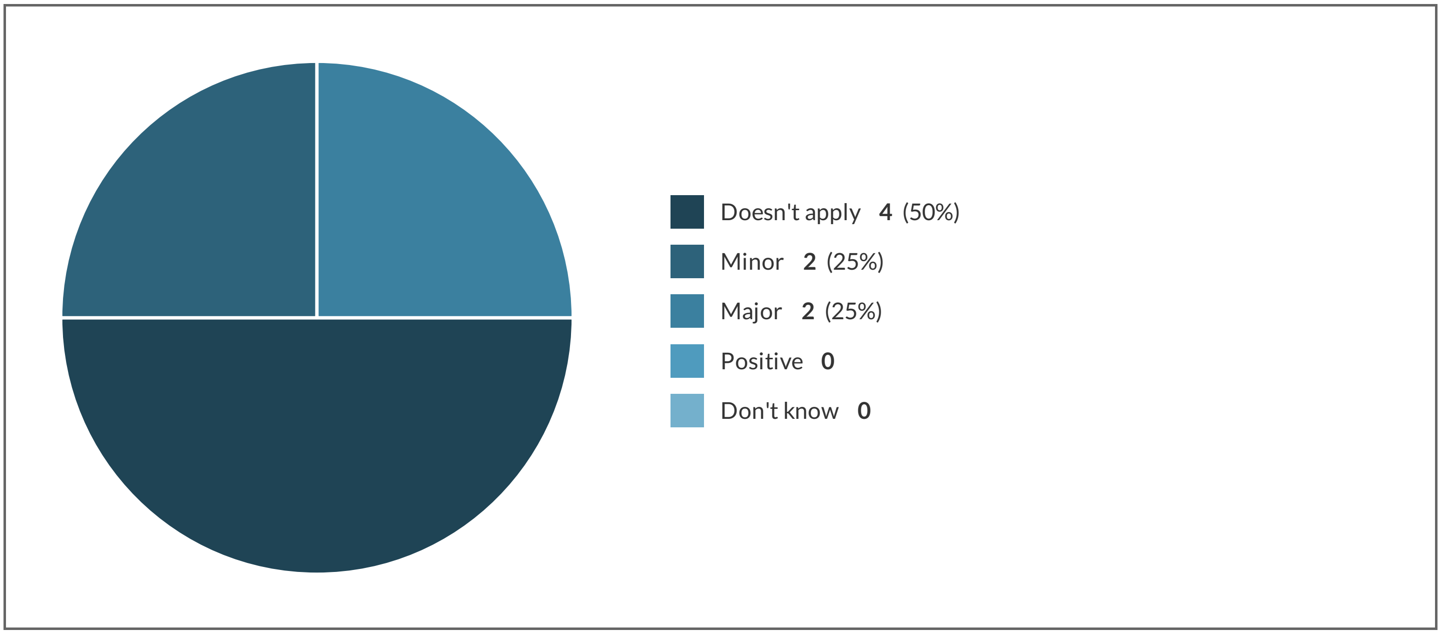


15.3.b Organization needs extra resources - Frequency Cost is Experienced

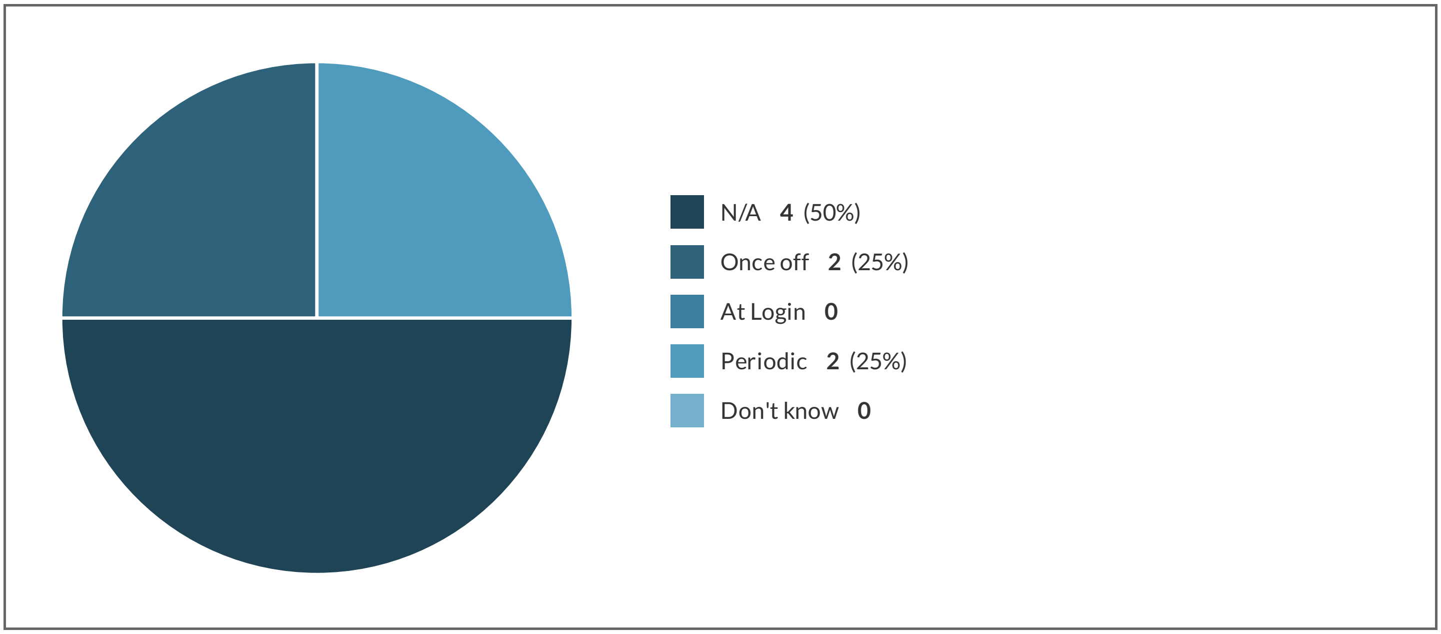


15.4 Takes organization time to implement

15.4.a Takes organization time to implement - Severity of Cost

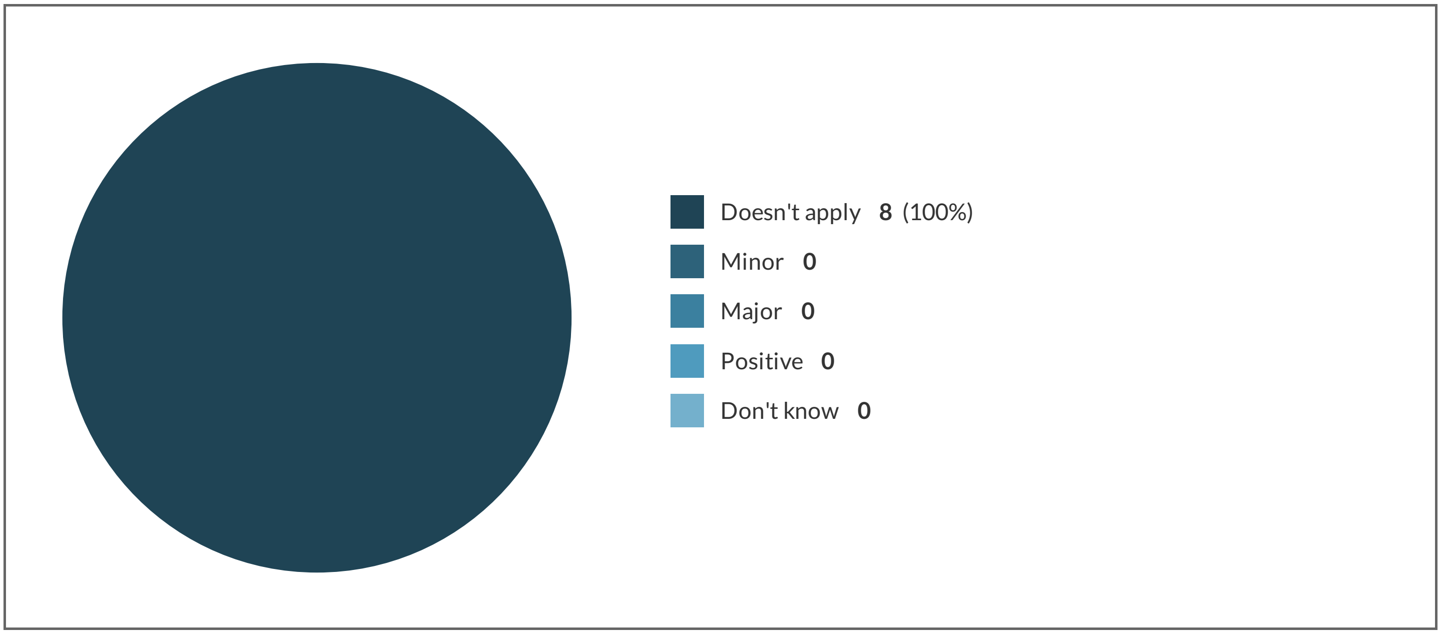


15.4.b Takes organization time to implement - Frequency Cost is Experienced

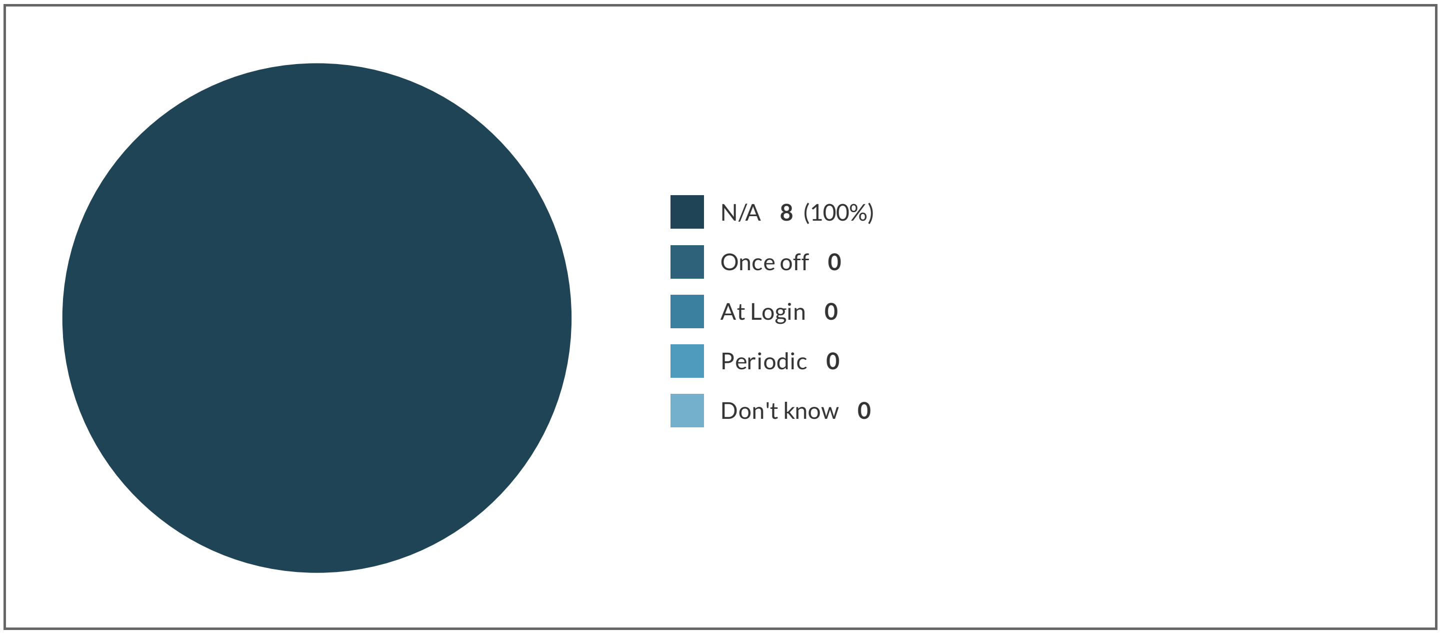


15.5 Increases the organization's computing power needed

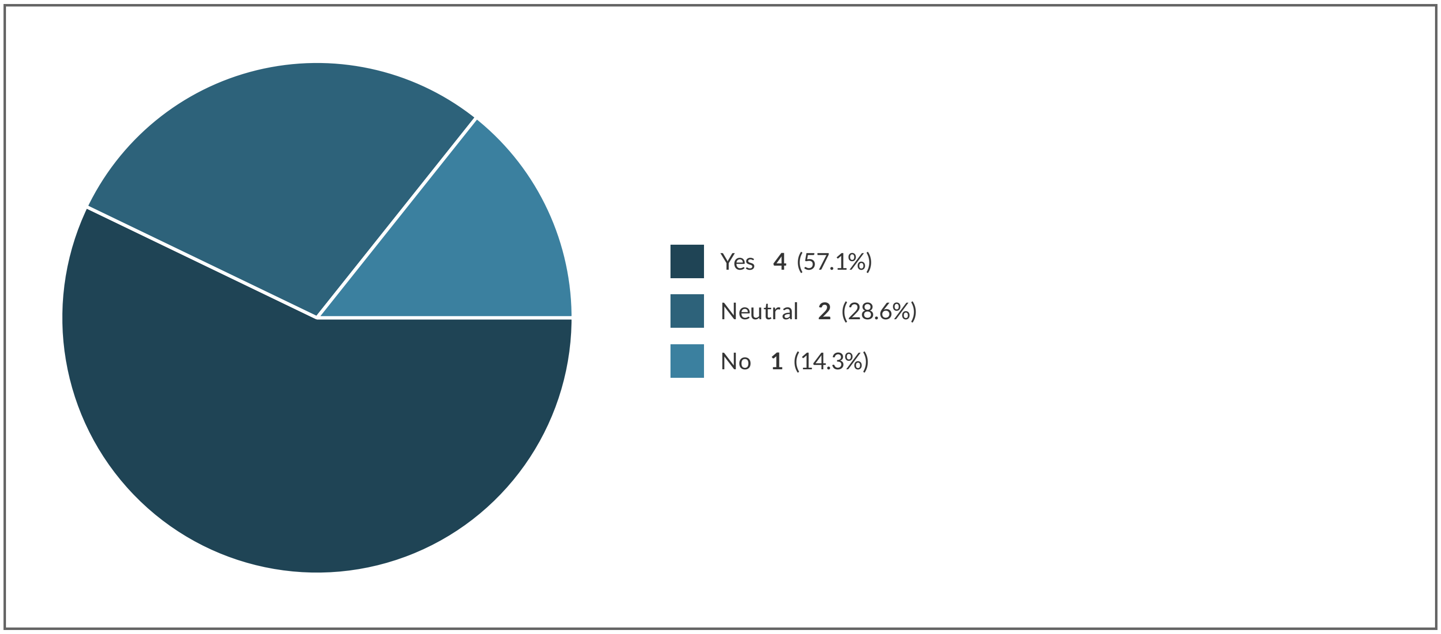
15.5.a Increases the organization's computing power needed - Severity of Cost



15.5.b Increases the organization's computing power needed - Frequency Cost is Experienced



15.a Do you approve of this advice?

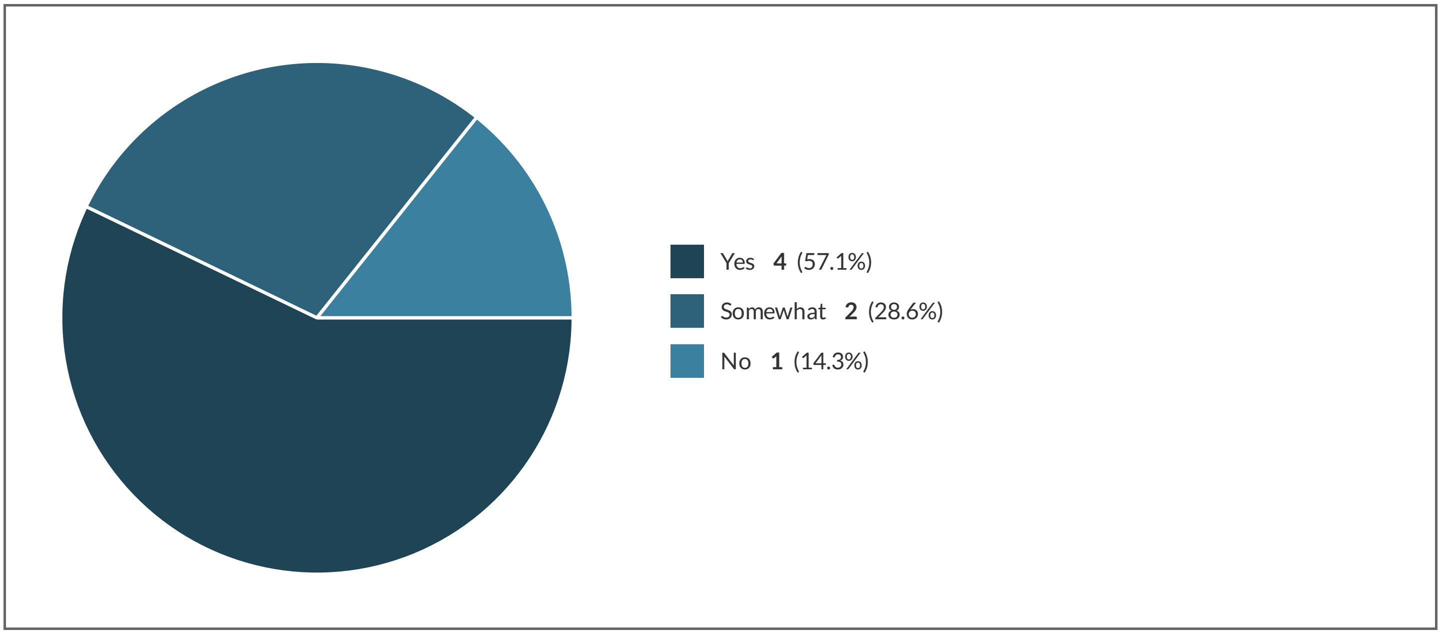


15.b Comments

Showing all 5 responses	
Just no. This remains a terrible idea.	634211-634202-66090277
we request in person with id	634211-634202-66098698
I'm for this idea but majority of companies nowadays are pushing for 100% paperless and "Go Digital" there has to be a digital method of sharing passwords securely	634211-634202-66754804
I think it would be more important to make sure that the passwords need to be changed on first login but I mean it can't hurt to conceal them in some way.	634211-634202-66754952
Sealed envelopes are not required sending parts of a password by seperare services can work, part by email without data on the characters meaning, part via SMS, part over Voice etc.	634211-634202-66871889

Final Comments

16 Do you agree with the five cost categories that were used to denote organization/administration costs in this survey?



16.a Are there any cost categories that you think should be added or removed?

Showing all 3 responses	
User time - how much of a burden is placed on the user who just wants to login. People are the weakest link, if security is seen as a burden they will seek shortcuts.	634211-634202-66090277
“Resources” is not specific enough	634211-634202-66532254
Some costs referred as minor would be better served by minimal or negligible. Everything has a cost sometimes it is small, but in may areas questioned in this survey, the benefit outweighs the cost.	634211-634202-66871889

17 This is the end of the survey do you have any final comments?

Showing 1 response

We're only as secure as our least secure password. You can have every precaution under the sun but if Bob from finance is using p@ssw0rd as his password and isn't using MFA you're going to lose all of your financial records.

Bit of background on myself, while I'm not directly involved on the day to day of managing users and passwords, I am a developer who has written many Authorization and Authentication systems over the years and as you can probably tell I have become pretty opinionated about it.

Education is incredibly important when it comes to password creation and password management. I believe nowadays at a bare minimum the following should be mandatory

1. Password Length (I would say at least 16 characters but people will disagree with me on that)
2. Multi-Factor Authentication: Push notification or a OTP (One Time Password)

If we're talking internal to a company here I believe employers should provide a subscription to something like LastPass or OnePassword and provide education on how to use it properly. Both of those pieces of software can generate random passwords of gibberish of a specified length and I'm not sure about LastPass but OnePassword can also generate a memorable and secure password of a specified length. Both can also manage OTPs for MFA as well which is just handy.

I also believe a company should maintain a "Common Password" list and automatically bar them from being used (using a common password dictionary is a common tactic of attackers) or if they don't want to maintain their own they can integrate with a service like haveibeenpwned (HIPB) run by Troy Hunt who anyone concerned with security should be following imo.

From a B2C (Business to Consumer) sense the business should be doing their best to promote MFA and maintaining a list of banned "Common Passwords" (or once again integrating with HIBP) granted you have less control over the random users that stumble on your site.

I wont get too much into my hatred for composition policies again but I will leave a link to this XKCD comic which kind of sums it up: https://xkcd.com/936/

Hope my ramblings could be of some help.

634211-634202-66754952