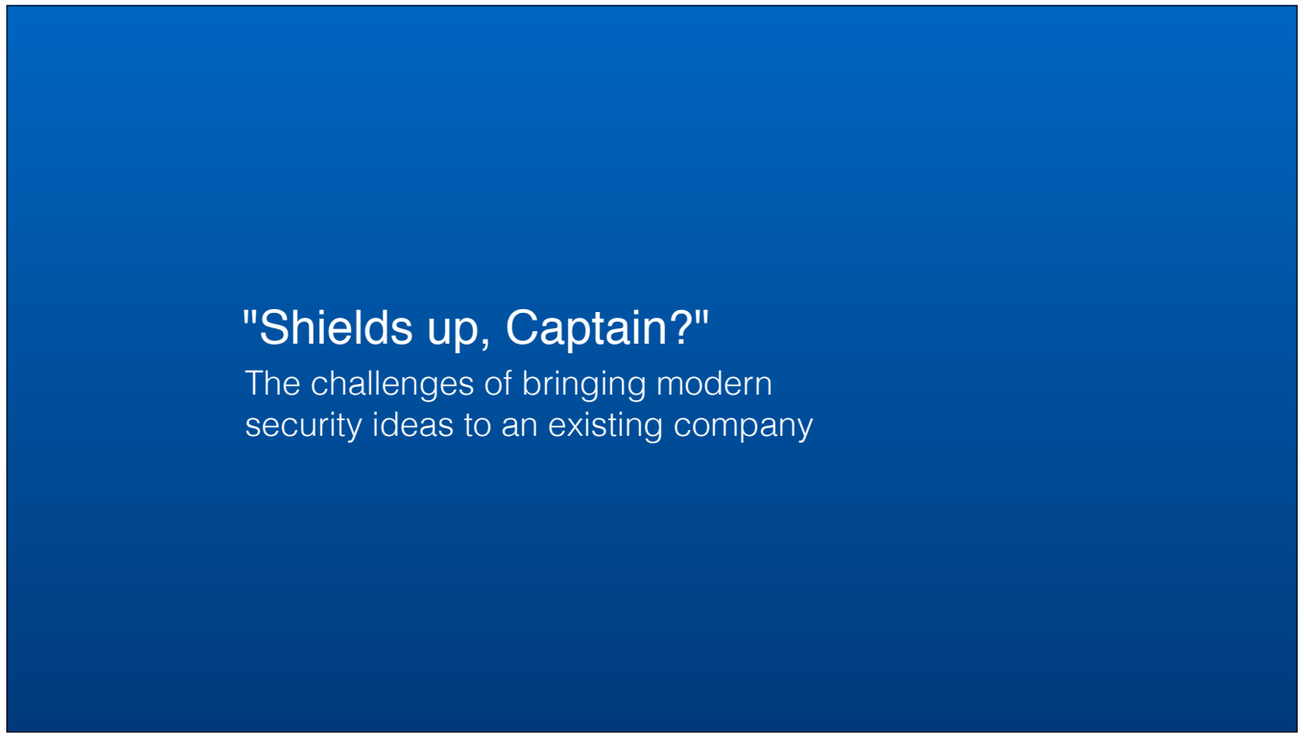
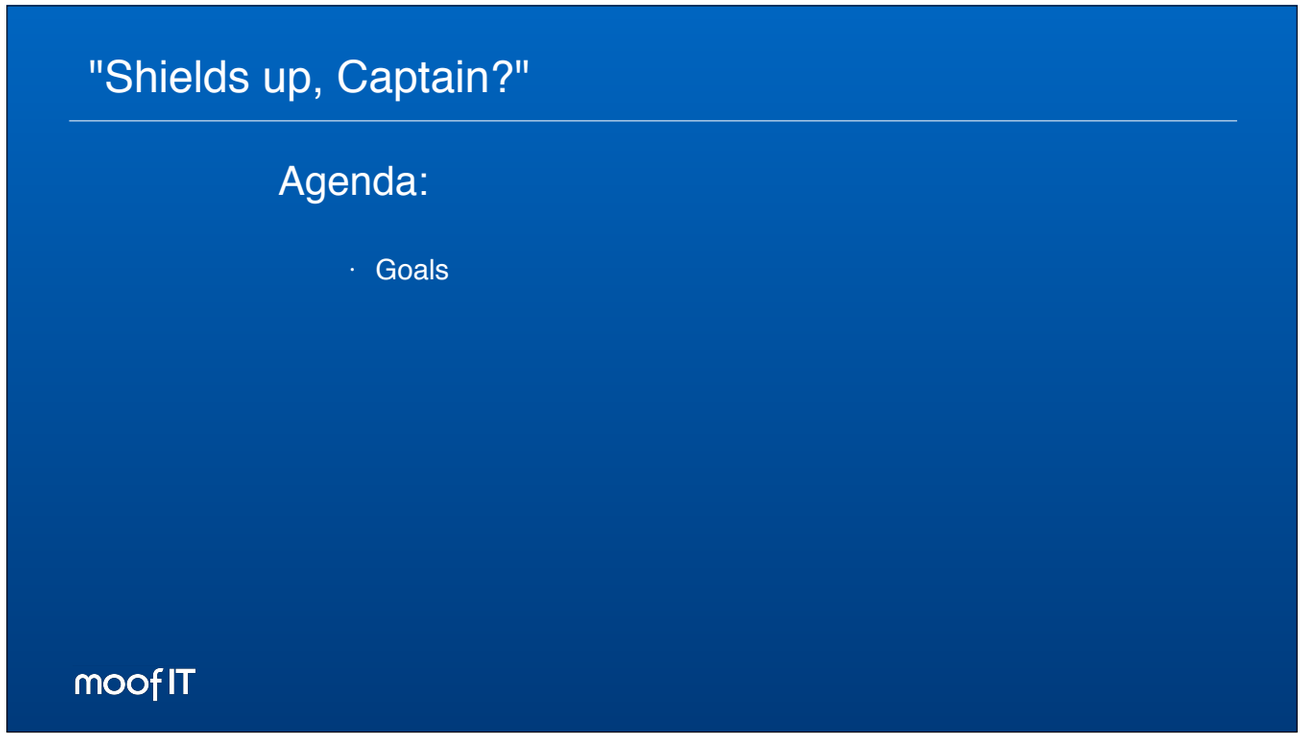

moof IT

Hi and Welcome to MacADUK 2018.
My name is Darren Wallace and I'm an Apple Consultant for Moof IT (and previously Amsys).
Some background: Combined I've been working with Apple products for over 12 years, starting as a Hardware repair trainee, to my current role as an Apple Consultant and for the last year or two, I've also helped out at the London Apple Admins meetups.
At Moof IT, we're a support and services company providing outsourced MSP and escalated support to various clients.
You can find me on Slack and twitter and most other things as daz_wallace



This is my first conference talk, so sorry in advance for the number of 'erms' and 'arrs' but I'll try and keep them to a minimum as best I can.
Over the summer, I worked with a customer on increasing the level of security for their IT solutions.
In this session I'll be looking to cover some of the challenges I faced, including the more human aspects I came across, as well as the techie challenges too.
Some general points:

- Slides will be available after the conference, on the Moof-IT blog page.
- Please hold any questions to the end. If I run out of time for a Q and A, feel free to grab me at any point during the conference, or via Slack or Twitter.
- I've added a few URLs to the keynote, but these will also be added to the blog. The URL at the very end will link to the blog post.



Firstly the agenda:

- Goals - Going over what the targets and goals of the project actually were

CLICK

- Plan - The rough plan for implementing the changes

CLICK

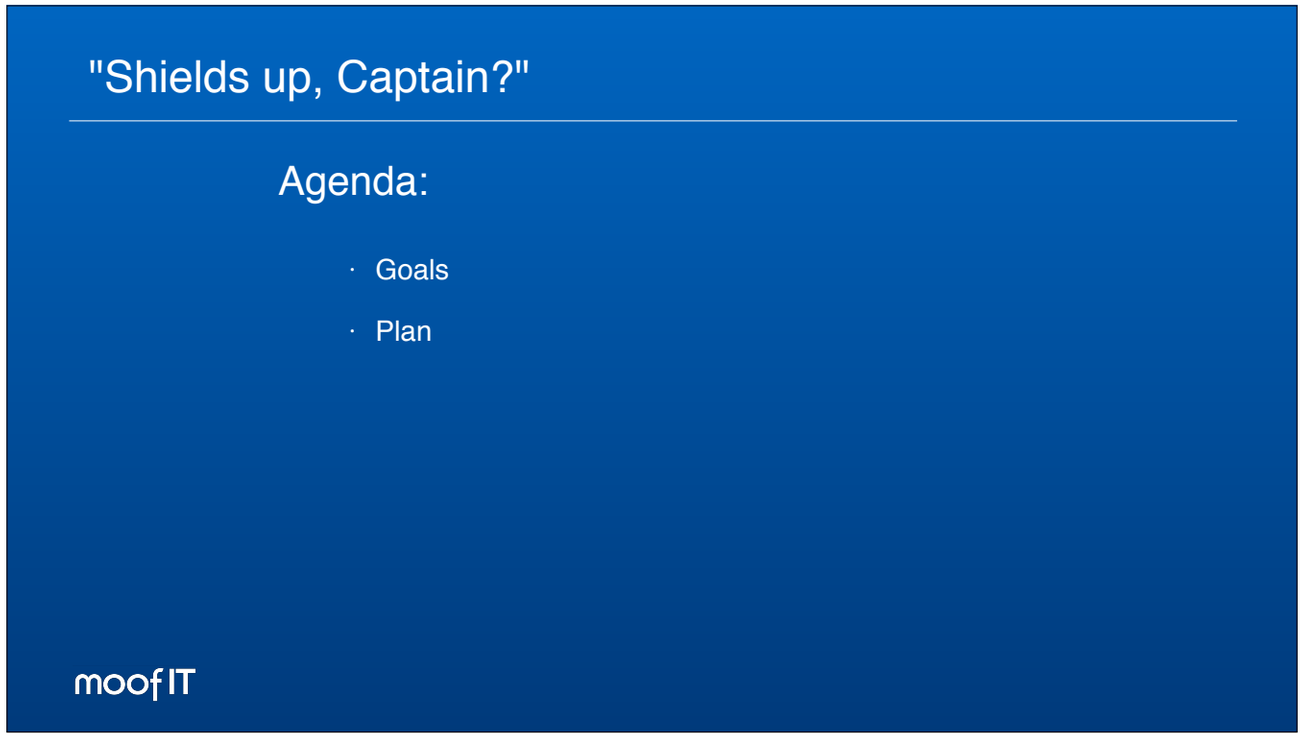
- Snags - Technical and Human - Nothing ever goes 100% to plan, and I'll go over some of the technical and human challenges I came across

CLICK

- Lessons learned - Taking all the snags and lessons learnt from the project, and turning those into advice and tips I can share with you all today.

CLICK

- Looking to the future - What's next for the project?



Firstly the agenda:

- Goals - Going over what the targets and goals of the project actually were

CLICK

- Plan - The rough plan for implementing the changes

CLICK

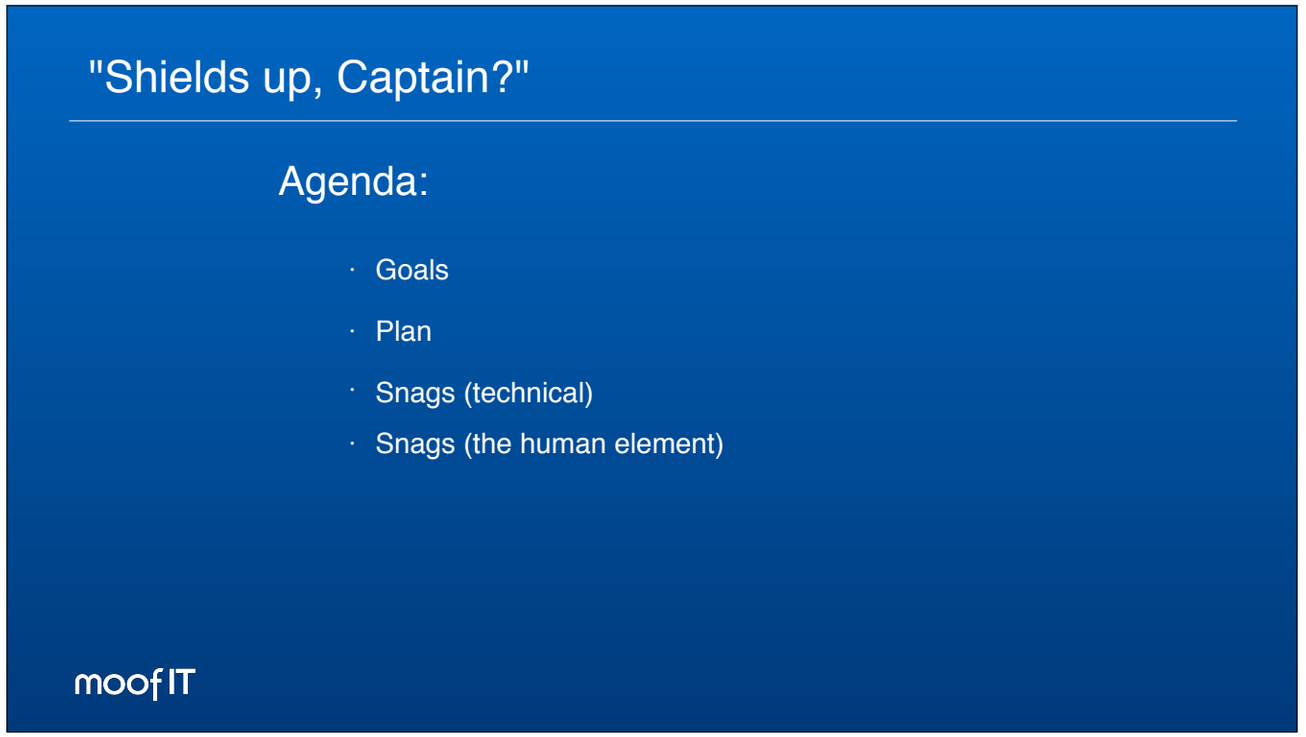
- Snags - Technical and Human - Nothing ever goes 100% to plan, and I'll go over some of the technical and human challenges I came across

CLICK

- Lessons learned - Taking all the snags and lessons learnt from the project, and turning those into advice and tips I can share with you all today.

CLICK

- Looking to the future - What's next for the project?



Firstly the agenda:

- Goals - Going over what the targets and goals of the project actually were

CLICK

- Plan - The rough plan for implementing the changes

CLICK

- Snags - Technical and Human - Nothing ever goes 100% to plan, and I'll go over some of the technical and human challenges I came across

CLICK

- Lessons learned - Taking all the snags and lessons learnt from the project, and turning those into advice and tips I can share with you all today.

CLICK

- Looking to the future - What's next for the project?

Firstly the agenda:

- Goals - Going over what the targets and goals of the project actually were

CLICK

- Plan - The rough plan for implementing the changes

CLICK

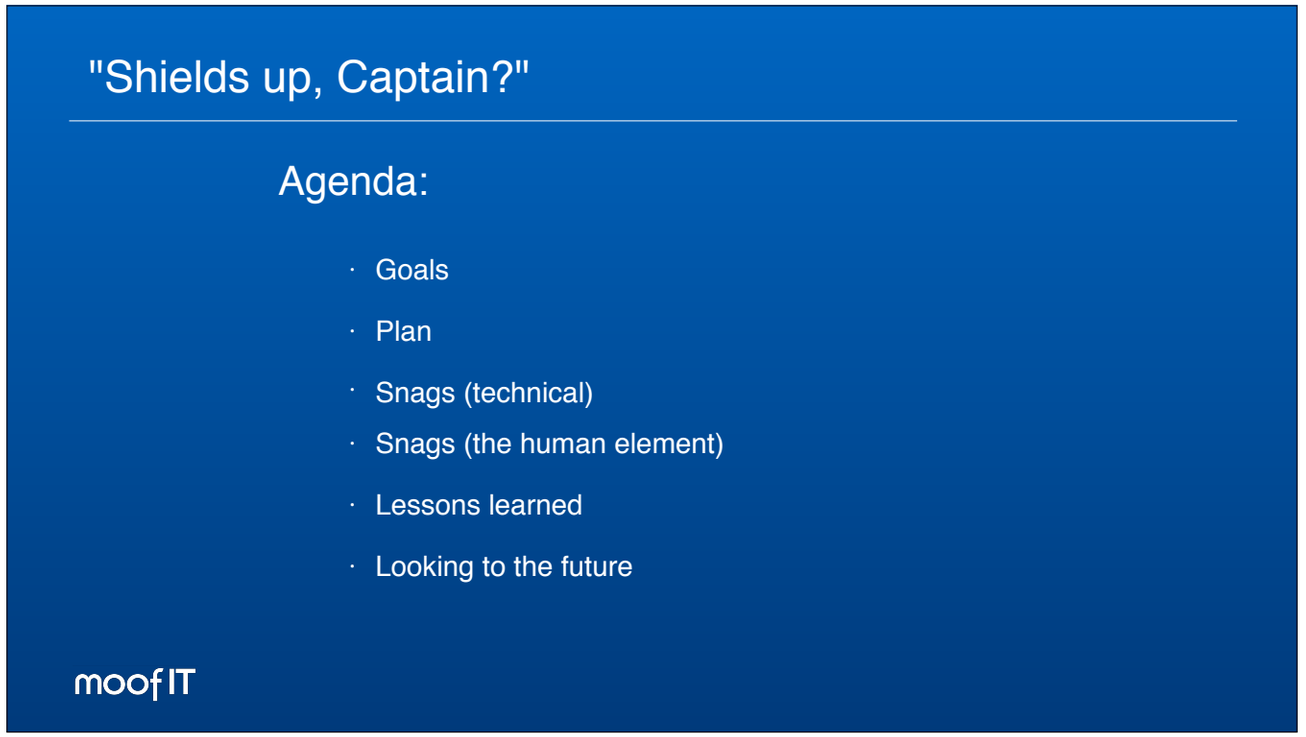
- Snags - Technical and Human - Nothing ever goes 100% to plan, and I'll go over some of the technical and human challenges I came across

CLICK

- Lessons learned - Taking all the snags and lessons learnt from the project, and turning those into advice and tips I can share with you all today.

CLICK

- Looking to the future - What's next for the project?



Firstly the agenda:

- Goals - Going over what the targets and goals of the project actually were

CLICK

- Plan - The rough plan for implementing the changes

CLICK

- Snags - Technical and Human - Nothing ever goes 100% to plan, and I'll go over some of the technical and human challenges I came across

CLICK

- Lessons learned - Taking all the snags and lessons learnt from the project, and turning those into advice and tips I can share with you all today.

CLICK

- Looking to the future - What's next for the project?

Goals

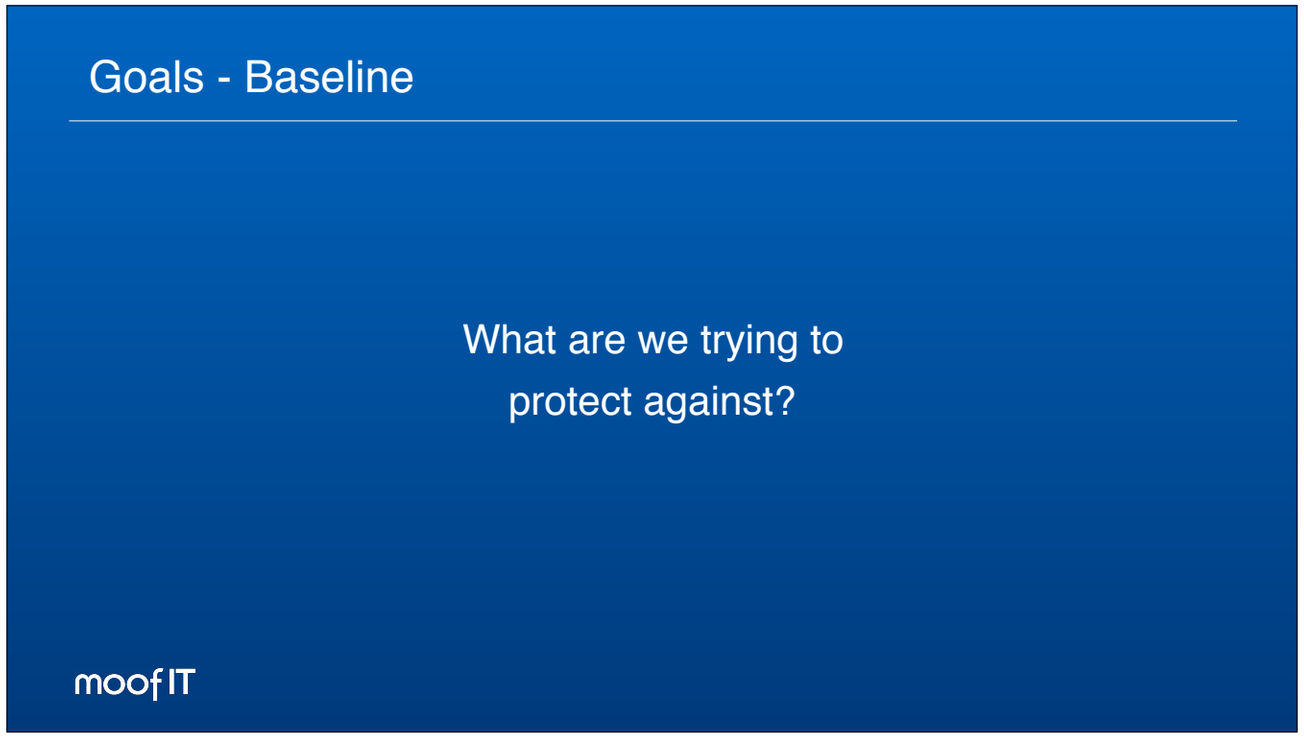
Right, The goals.

Before we start the work, we needed to find out what the actual goals of the project would be.
Without at least some goals set, we wouldn't know if what we're doing is the right direction to go in, or even when we would be successful

Goals

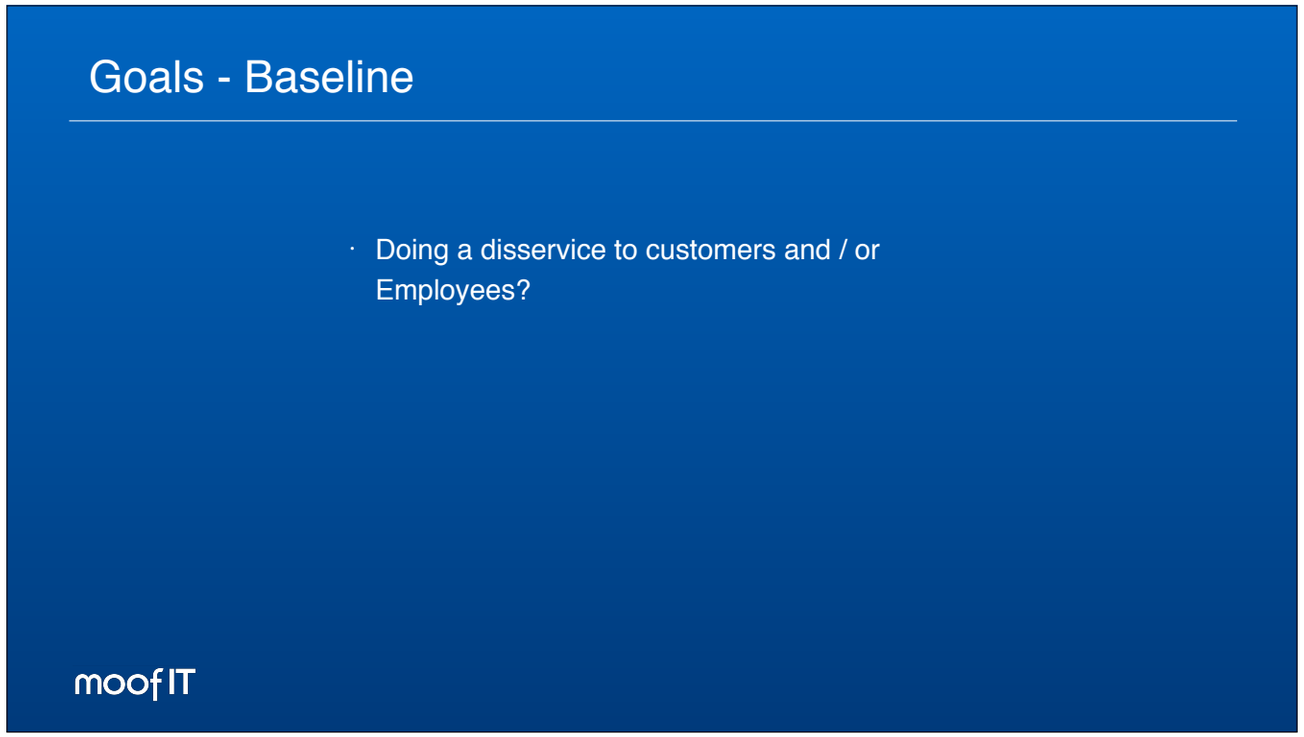
Right, The goals.

Before we start the work, we needed to find out what the actual goals of the project would be.
Without at least some goals set, we wouldn't know if what we're doing is the right direction to go in, or even when we would be successful



So firstly we need to take a step back, and figure out what we mean by 'increasing the security' of a company.

The easiest Question is what are we trying to protect against?



Doing a disservice, or 'doing wrong' by customers and / or employees?

- This is one companies struggle with as it's more of a moral choice... that is unless they get publicly caught out!
- Don't forget, a company will not just hold data on customers, but employees' too (i.e. You!). Often this can be much more personal than customer information, especially if your employer works only with other companies. e.g. Home addresses? Personal Bank Details?

CLICK

What about being 'Hacked'?

- It's often the case nowadays that it'll be a more of when, not **If** you'll be 'hacked'.
- Does this mean there's nothing that can be done to reduce the risks? Or to better deal with the situation should they arise?

CLICK

Being sued or fined?

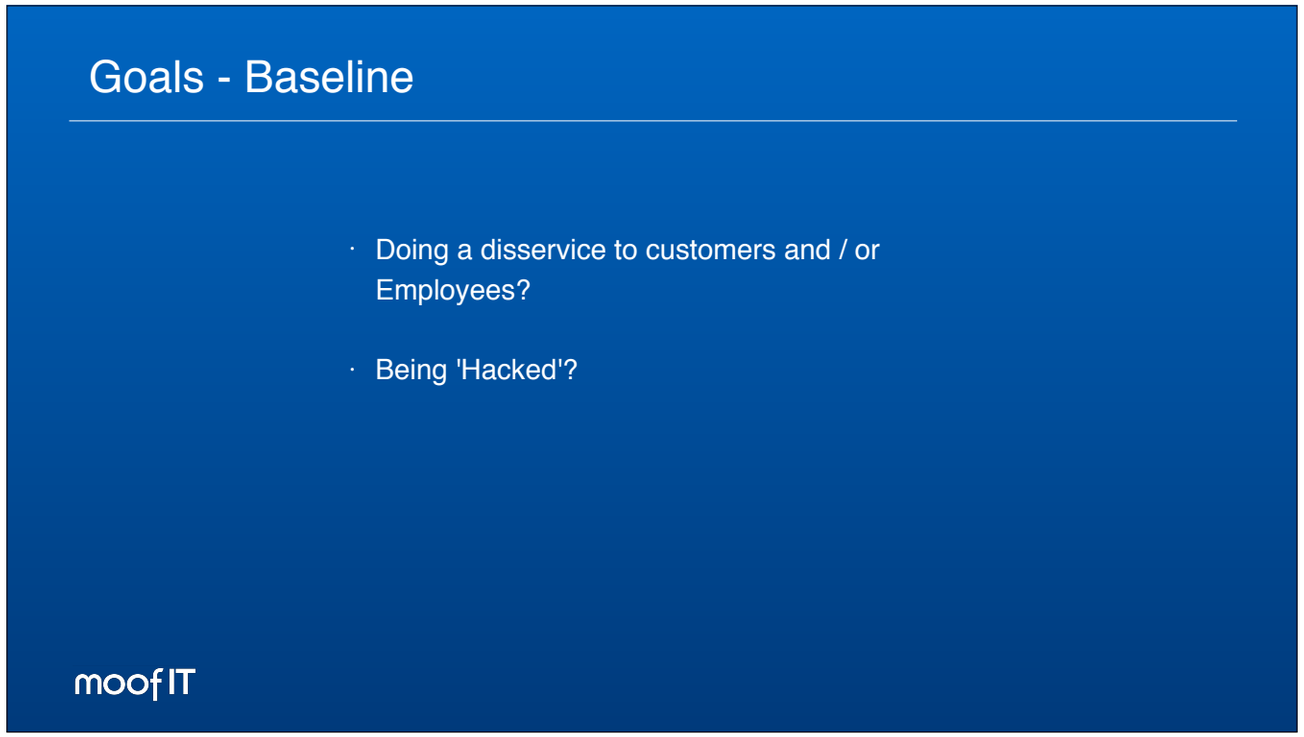
- This tends to be a massive one for a company as it costs them money, their bottom line.
- This normally is as a result of non-compliancy with industry regulations (such as in finance) or government regulations (such as GDPR in the UK - everyone ready for the 25th May?)

CLICK

What about being infected?

- This one partly overlaps with being 'hacked'. It tends to more directly cause downtime. Either by ransomware or indirectly by having to take devices and services offline to cleanse them.

- And business downtime == money lost.



Doing a disservice, or 'doing wrong' by customers and / or employees?

- This is one companies struggle with as it's more of a moral choice... that is unless they get publicly caught out!
- Don't forget, a company will not just hold data on customers, but employees' too (i.e. You!). Often this can be much more personal than customer information, especially if your employer works only with other companies. e.g. Home addresses? Personal Bank Details?

CLICK

What about being 'Hacked'?

- It's often the case nowadays that it'll be a more of when, not **If** you'll be 'hacked'.
- Does this mean there's nothing that can be done to reduce the risks? Or to better deal with the situation should they arise?

CLICK

Being sued or fined?

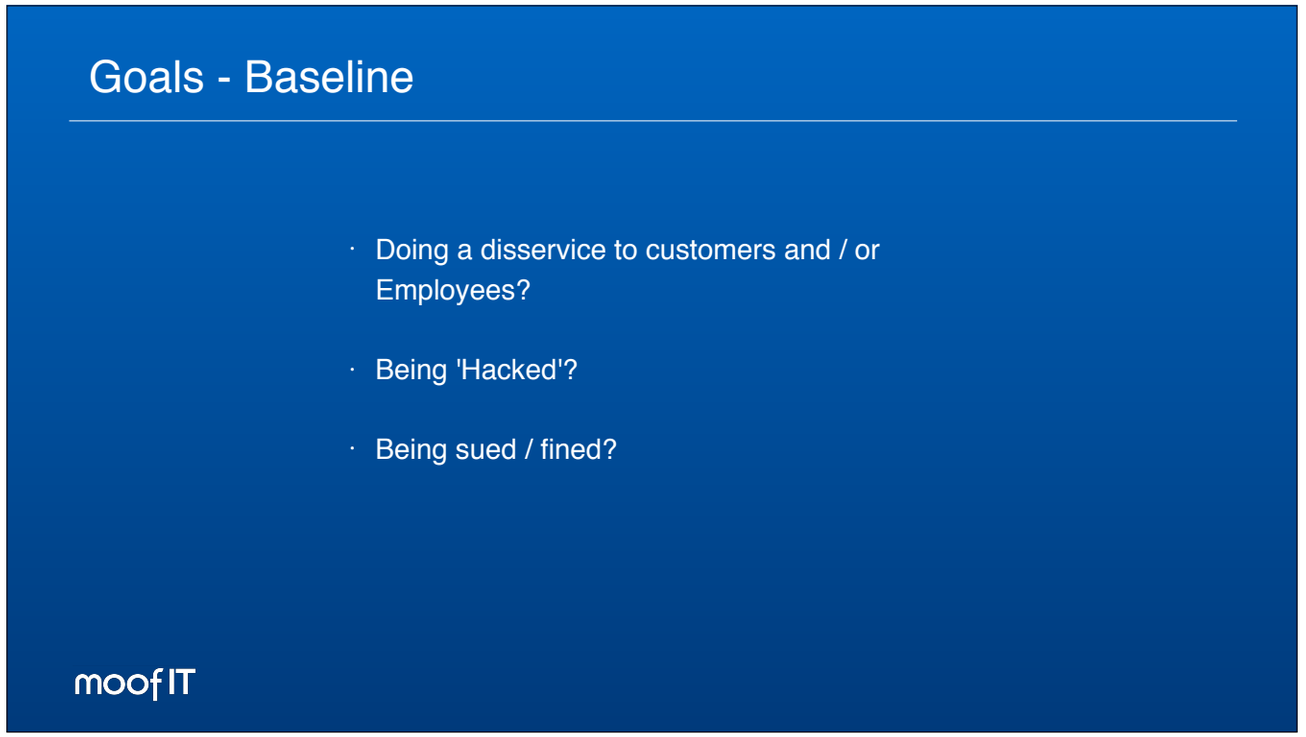
- This tends to be a massive one for a company as it costs them money, their bottom line.
- This normally is as a result of non-compliancy with industry regulations (such as in finance) or government regulations (such as GDPR in the UK - everyone ready for the 25th May?)

CLICK

What about being infected?

- This one partly overlaps with being 'hacked'. It tends to more directly cause downtime. Either by ransomware or indirectly by having to take devices and services offline to cleanse them.

- And business downtime == money lost.



Doing a disservice, or 'doing wrong' by customers and / or employees?

- This is one companies struggle with as it's more of a moral choice... that is unless they get publicly caught out!
- Don't forget, a company will not just hold data on customers, but employees' too (i.e. You!). Often this can be much more personal than customer information, especially if your employer works only with other companies. e.g. Home addresses? Personal Bank Details?

CLICK

What about being 'Hacked'?

- It's often the case nowadays that it'll be a more of when, not **If** you'll be 'hacked'.
- Does this mean there's nothing that can be done to reduce the risks? Or to better deal with the situation should they arise?

CLICK

Being sued or fined?

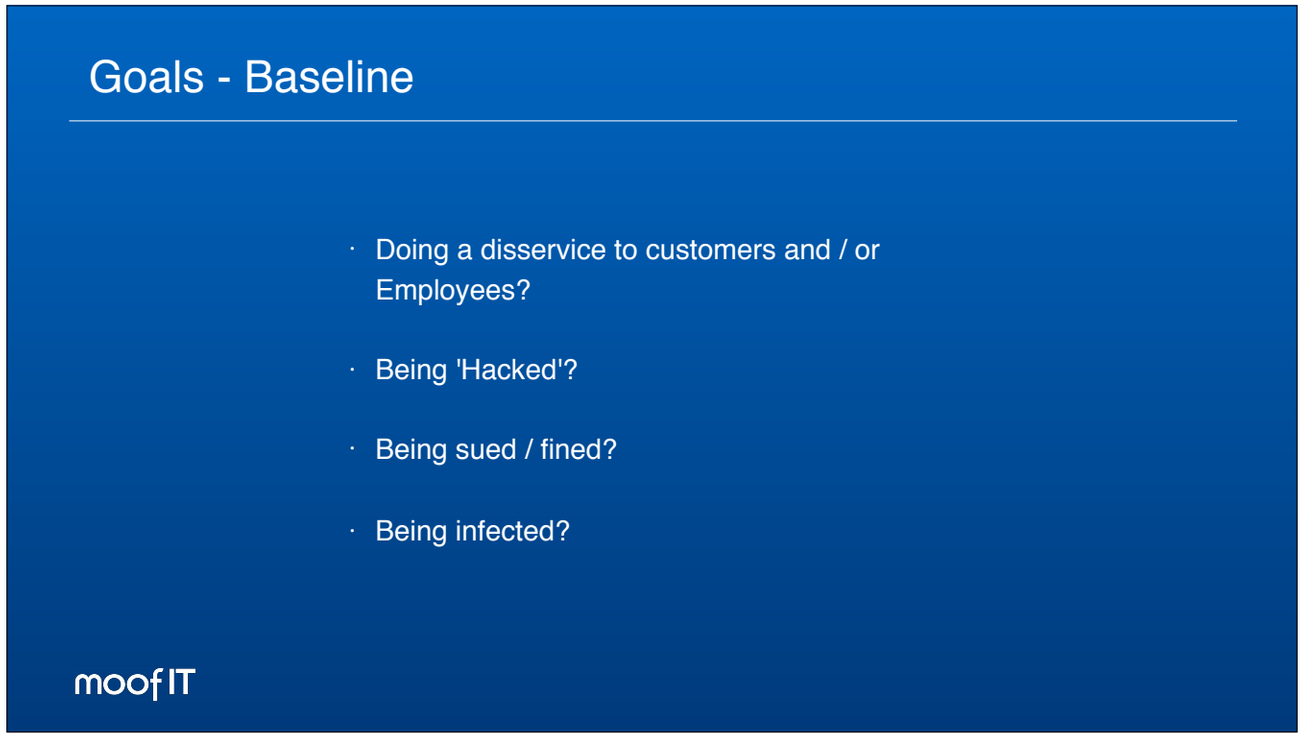
- This tends to be a massive one for a company as it costs them money, their bottom line.
- This normally is as a result of non-compliancy with industry regulations (such as in finance) or government regulations (such as GDPR in the UK - everyone ready for the 25th May?)

CLICK

What about being infected?

- This one partly overlaps with being 'hacked'. It tends to more directly cause downtime. Either by ransomware or indirectly by having to take devices and services offline to cleanse them.

- And business downtime == money lost.



Doing a disservice, or 'doing wrong' by customers and / or employees?

- This is one companies struggle with as it's more of a moral choice... that is unless they get publicly caught out!
- Don't forget, a company will not just hold data on customers, but employees' too (i.e. You!). Often this can be much more personal than customer information, especially if your employer works only with other companies. e.g. Home addresses? Personal Bank Details?

CLICK

What about being 'Hacked'?

- It's often the case nowadays that it'll be a more of when, not **If** you'll be 'hacked'.
- Does this mean there's nothing that can be done to reduce the risks? Or to better deal with the situation should they arise?

CLICK

Being sued or fined?

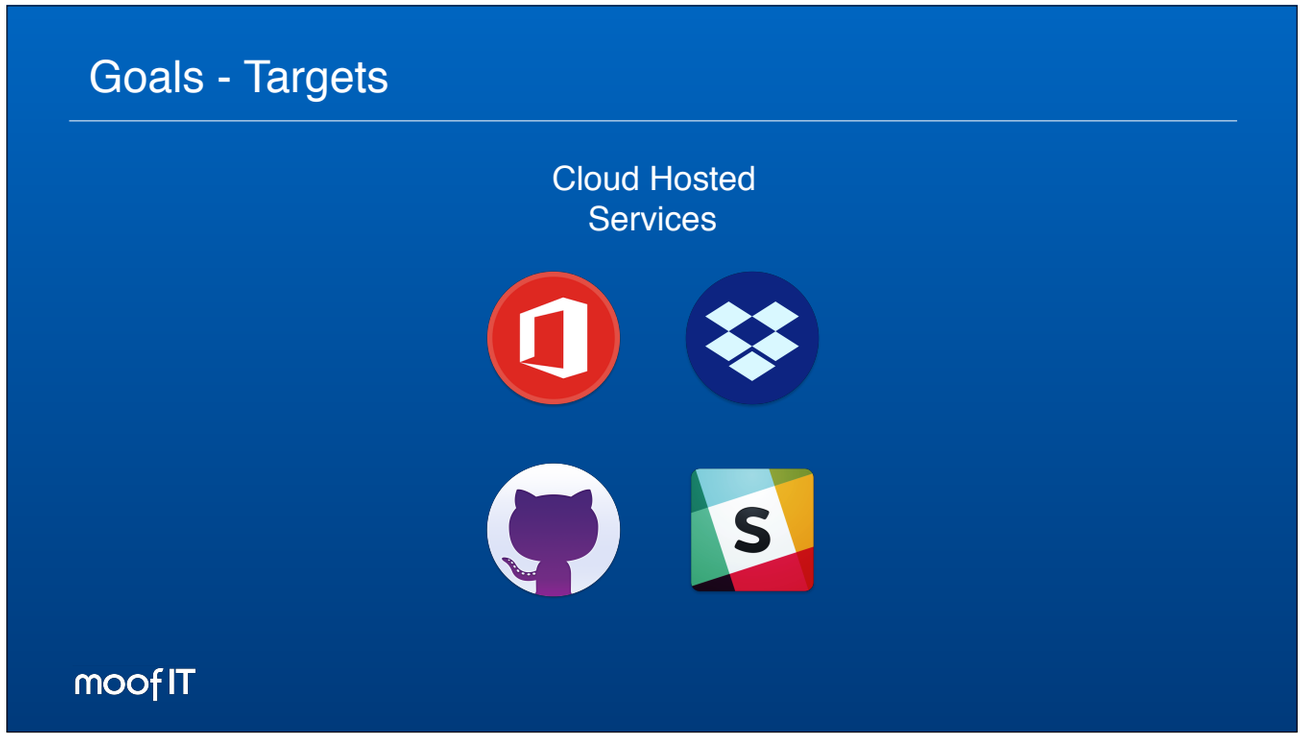
- This tends to be a massive one for a company as it costs them money, their bottom line.
- This normally is as a result of non-compliancy with industry regulations (such as in finance) or government regulations (such as GDPR in the UK - everyone ready for the 25th May?)

CLICK

What about being infected?

- This one partly overlaps with being 'hacked'. It tends to more directly cause downtime. Either by ransomware or indirectly by having to take devices and services offline to cleanse them.

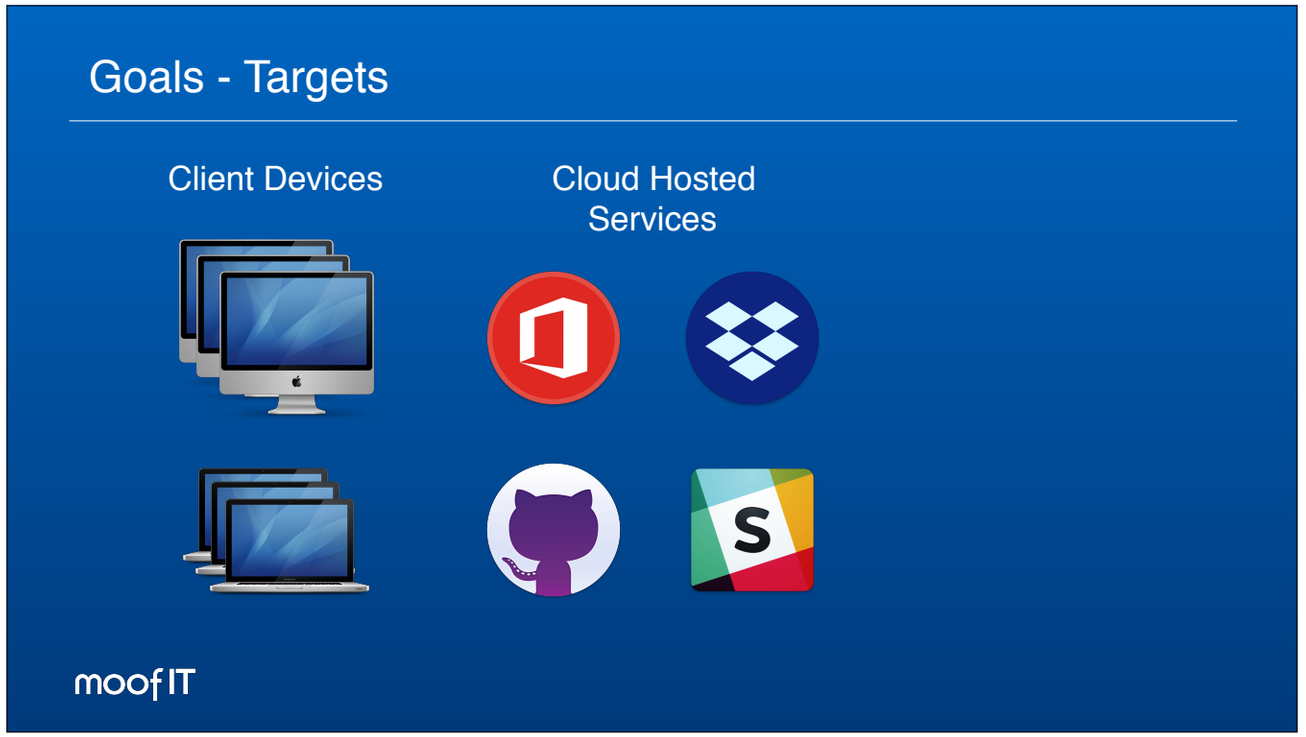
- And business downtime == money lost.



Now, we have our baseline, we have to define what areas we were working with.
For this project we split the targets into 3 areas:
CLICK
- Client endpoints (in this case macOS devices)
    - Mac laptops and desktops
    - These were all in current use, and things like wipe and redeploy were not an option

CLICK
- Cloud hosted services
    - Including Office 365, Dropbox, GitHub and Slack amongst others

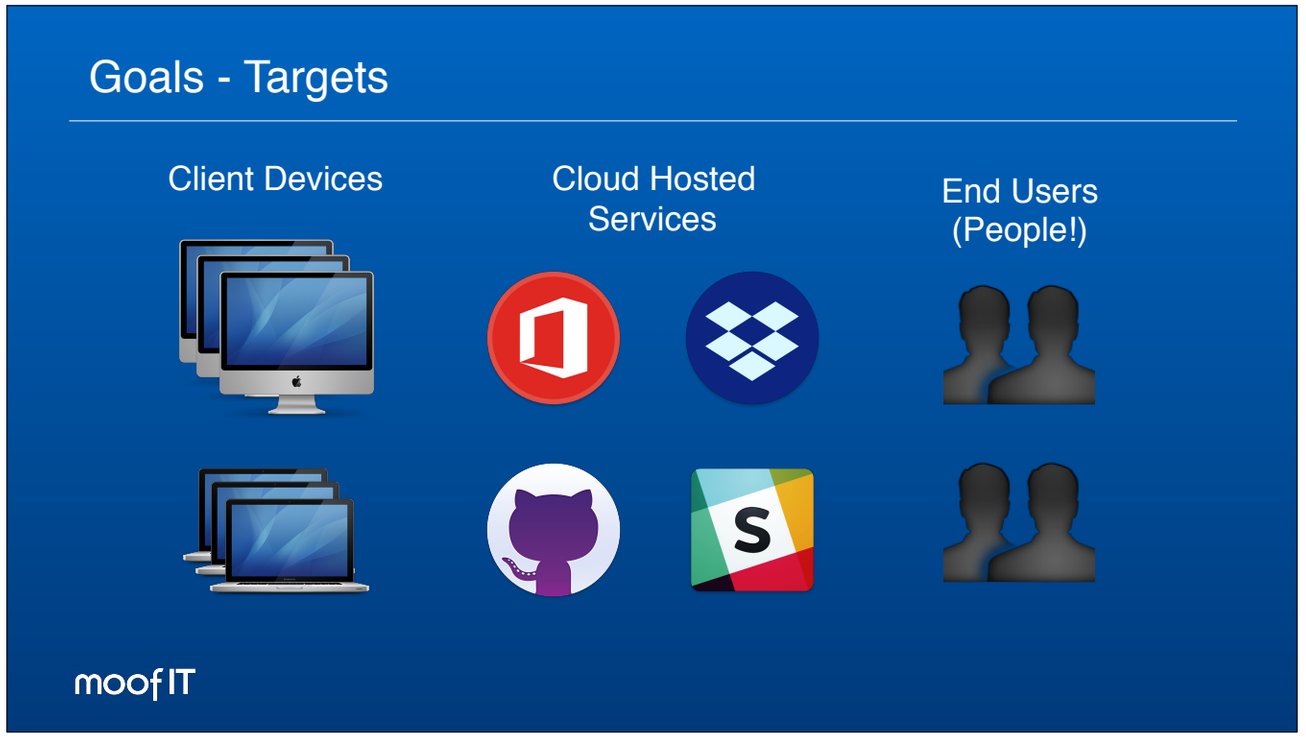
CLICK
- End Users
    - People, you know - like you or me!
    - The technical ability of these users ranged dramatically from 'very' (like you all here), through 'kinda / ish' (like generally younger generations, those grown up with their own computers and games consoles), right to 'almost zero' (they're great at customer interactions or a daemon with Excel, but perhaps they struggle with some things we'd take for granted, like checking email, or accessing new systems).
        - I try to make a point to be extra helpful to these users. They may not be technically savvy, but they'd run rings around me all-day in their normal roles and tasks.



Now, we have our baseline, we have to define what areas we were working with.
For this project we split the targets into 3 areas:
CLICK
- Client endpoints (in this case macOS devices)
    - Mac laptops and desktops
    - These were all in current use, and things like wipe and redeploy were not an option

CLICK
- Cloud hosted services
    - Including Office 365, Dropbox, GitHub and Slack amongst others

CLICK
- End Users
    - People, you know - like you or me!
    - The technical ability of these users ranged dramatically from 'very' (like you all here), through 'kinda / ish' (like generally younger generations, those grown up with their own computers and games consoles), right to 'almost zero' (they're great at customer interactions or a daemon with Excel, but perhaps they struggle with some things we'd take for granted, like checking email, or accessing new systems).
        - I try to make a point to be extra helpful to these users. They may not be technically savvy, but they'd run rings around me all-day in their normal roles and tasks.



Now, we have our baseline, we have to define what areas we were working with.
For this project we split the targets into 3 areas:
CLICK

- Client endpoints (in this case macOS devices)
    - Mac laptops and desktops
    - These were all in current use, and things like wipe and redeploy were not an option

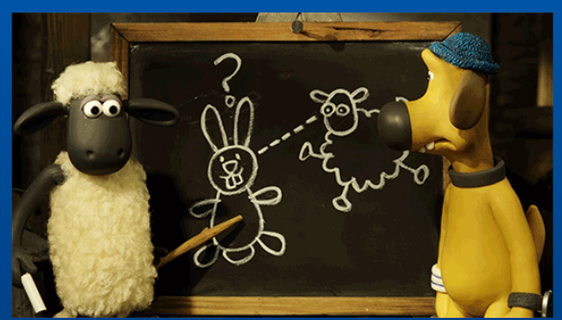
CLICK

- Cloud hosted services
    - Including Office 365, Dropbox, GitHub and Slack amongst others

CLICK

- End Users
    - People, you know - like you or me!
    - The technical ability of these users ranged dramatically from 'very' (like you all here), through 'kinda / ish' (like generally younger generations, those grown up with their own computers and games consoles), right to 'almost zero' (they're great at customer interactions or a daemon with Excel, but perhaps they struggle with some things we'd take for granted, like checking email, or accessing new systems).
        - I try to make a point to be extra helpful to these users. They may not be technically savvy, but they'd run rings around me all-day in their normal roles and tasks.

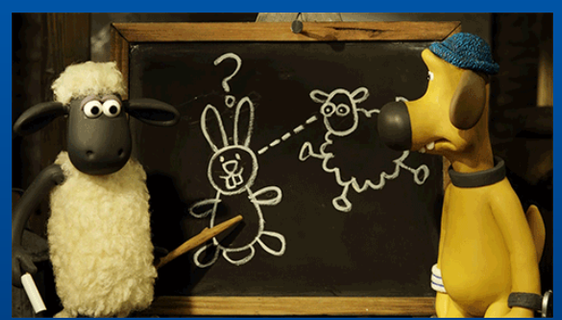
The Plan



So that's our targets defined, and a high-level baseline of what we are aiming for, what about a plan?

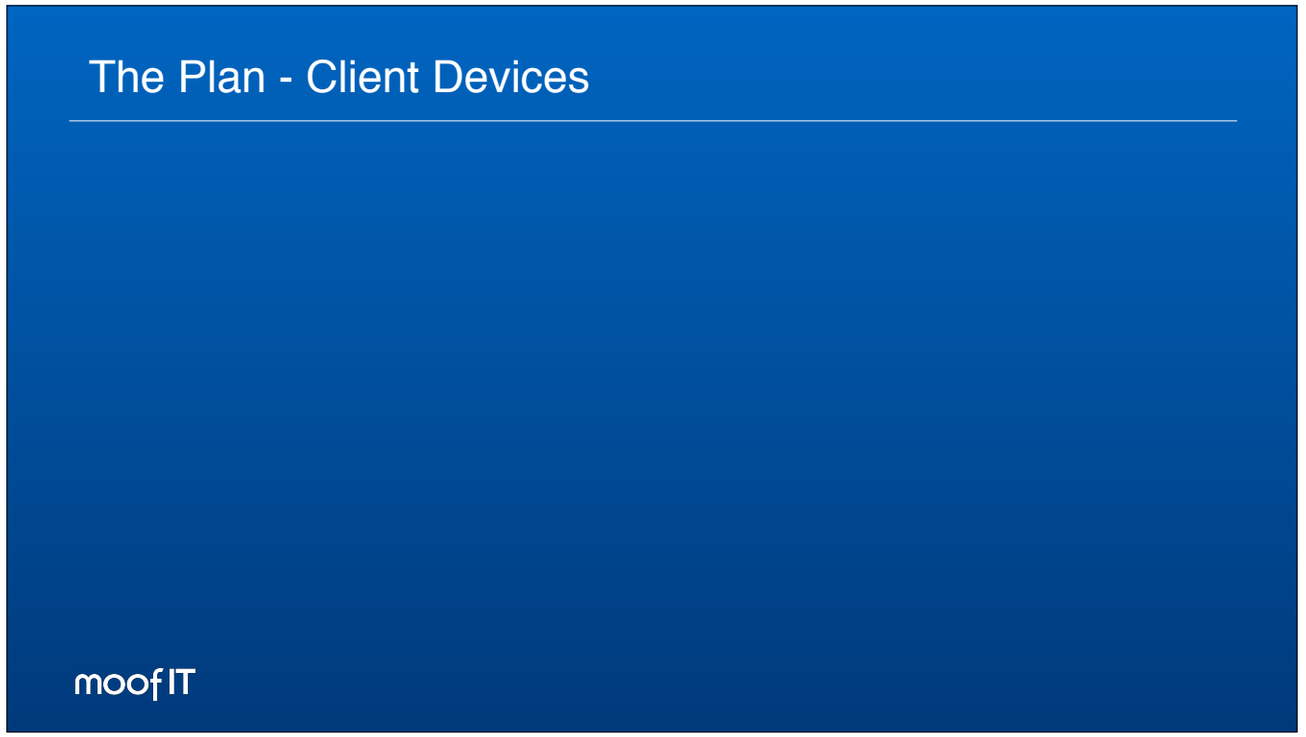
How are we gonna meet our baseline with our targets?

The Plan



So that's our targets defined, and a high-level baseline of what we are aiming for, what about a plan?

How are we gonna meet our baseline with our targets?

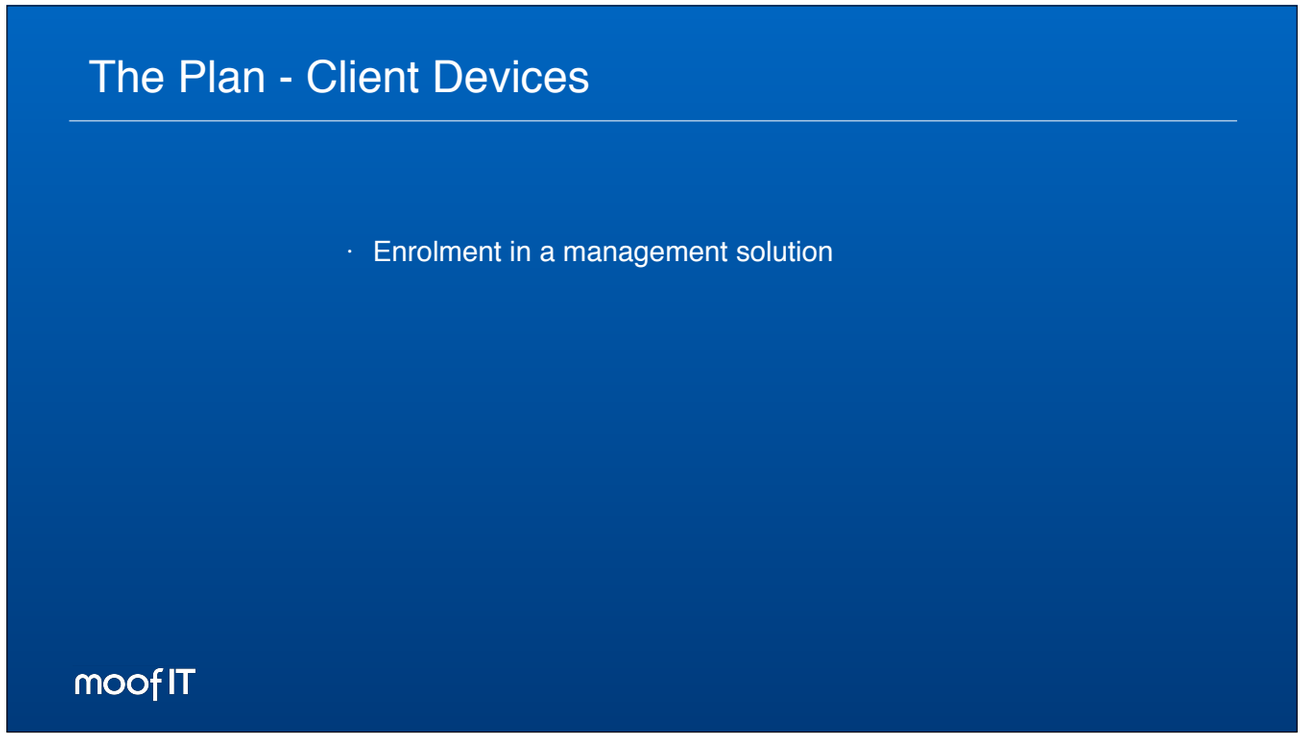


For the end devices we didn't want to completely lock down users. After-all, they're adults and employees, so we were not gonna to treat them as kids at school. In this spirit we were only looking to enforce what we felt was the minimum requirements to meet the baselines.
So the plan as far as the client devices go included:
CLICK
- Enrolment in a management solution
    - As a Jamf Partner and Integrator, we opted to use Jamf Pro as the solution here.

CLICK
- Full Disk encryption on all laptops
    - FileVault for this. As it's built into the OS, it was both the cheapest, and the least likely to have issues, especially with things like OS updates.

CLICK
- Password policies on devices:
    - As per the more recent advice from 'National Institute of Standards and Technology' (NIST), we're staying away from maximum password ages - aka "Change your password every 90 days"

CLICK
- Software patch policies with deadlines
    - Applications and OS updates



For the end devices we didn't want to completely lock down users. After-all, they're adults and employees, so we were not gonna to treat them as kids at school. In this spirit we were only looking to enforce what we felt was the minimum requirements to meet the baselines.
So the plan as far as the client devices go included:
CLICK
- Enrolment in a management solution
    - As a Jamf Partner and Integrator, we opted to use Jamf Pro as the solution here.

CLICK
- Full Disk encryption on all laptops
    - FileVault for this. As it's built into the OS, it was both the cheapest, and the least likely to have issues, especially with things like OS updates.

CLICK
- Password policies on devices:
    - As per the more recent advice from 'National Institute of Standards and Technology' (NIST), we're staying away from maximum password ages - aka "Change your password every 90 days"

CLICK
- Software patch policies with deadlines
    - Applications and OS updates

For the end devices we didn't want to completely lock down users. After-all, they're adults and employees, so we were not gonna to treat them as kids at school. In this spirit we were only looking to enforce what we felt was the minimum requirements to meet the baselines.
So the plan as far as the client devices go included:
CLICK
- Enrolment in a management solution
    - As a Jamf Partner and Integrator, we opted to use Jamf Pro as the solution here.

CLICK
- Full Disk encryption on all laptops
    - FileVault for this. As it's built into the OS, it was both the cheapest, and the least likely to have issues, especially with things like OS updates.

CLICK
- Password policies on devices:
    - As per the more recent advice from 'National Institute of Standards and Technology' (NIST), we're staying away from maximum password ages - aka "Change your password every 90 days"

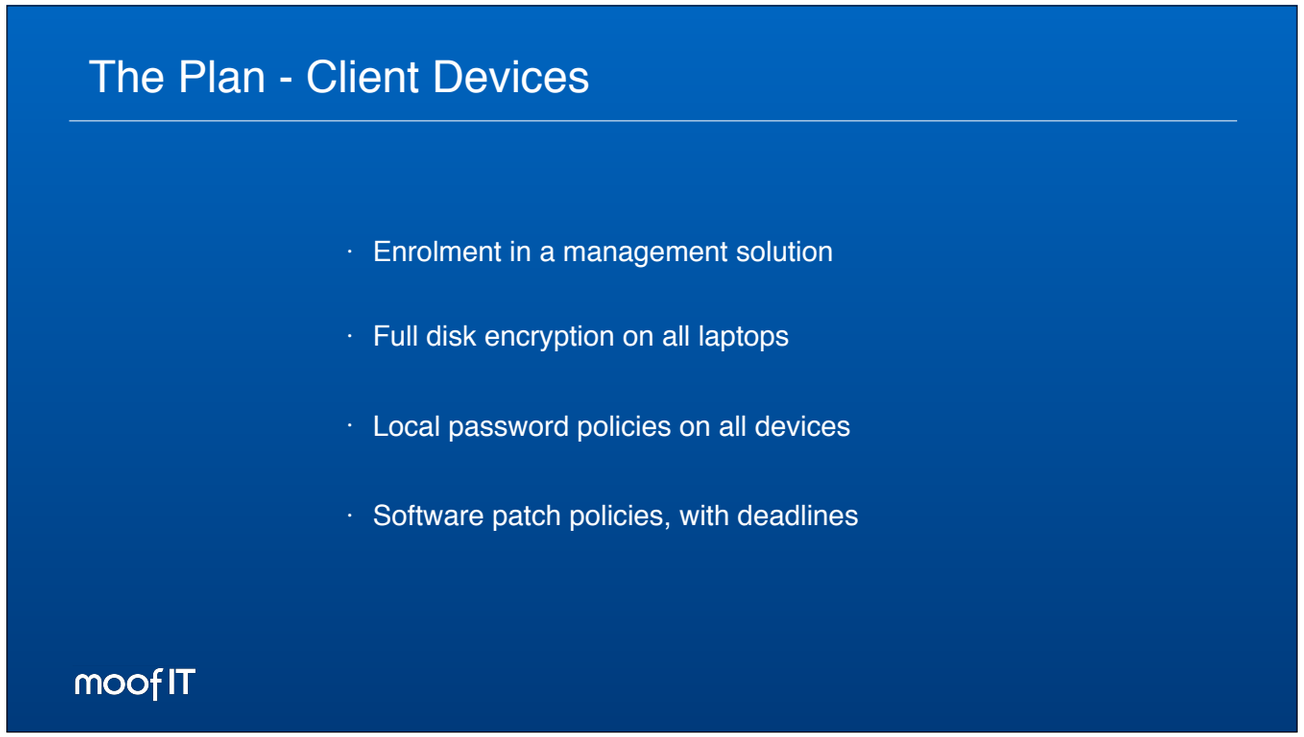
CLICK
- Software patch policies with deadlines
    - Applications and OS updates

For the end devices we didn't want to completely lock down users. After-all, they're adults and employees, so we were not gonna to treat them as kids at school. In this spirit we were only looking to enforce what we felt was the minimum requirements to meet the baselines.
So the plan as far as the client devices go included:
CLICK
- Enrolment in a management solution
    - As a Jamf Partner and Integrator, we opted to use Jamf Pro as the solution here.

CLICK
- Full Disk encryption on all laptops
    - FileVault for this. As it's built into the OS, it was both the cheapest, and the least likely to have issues, especially with things like OS updates.

CLICK
- Password policies on devices:
    - As per the more recent advice from 'National Institute of Standards and Technology' (NIST), we're staying away from maximum password ages - aka "Change your password every 90 days"

CLICK
- Software patch policies with deadlines
    - Applications and OS updates

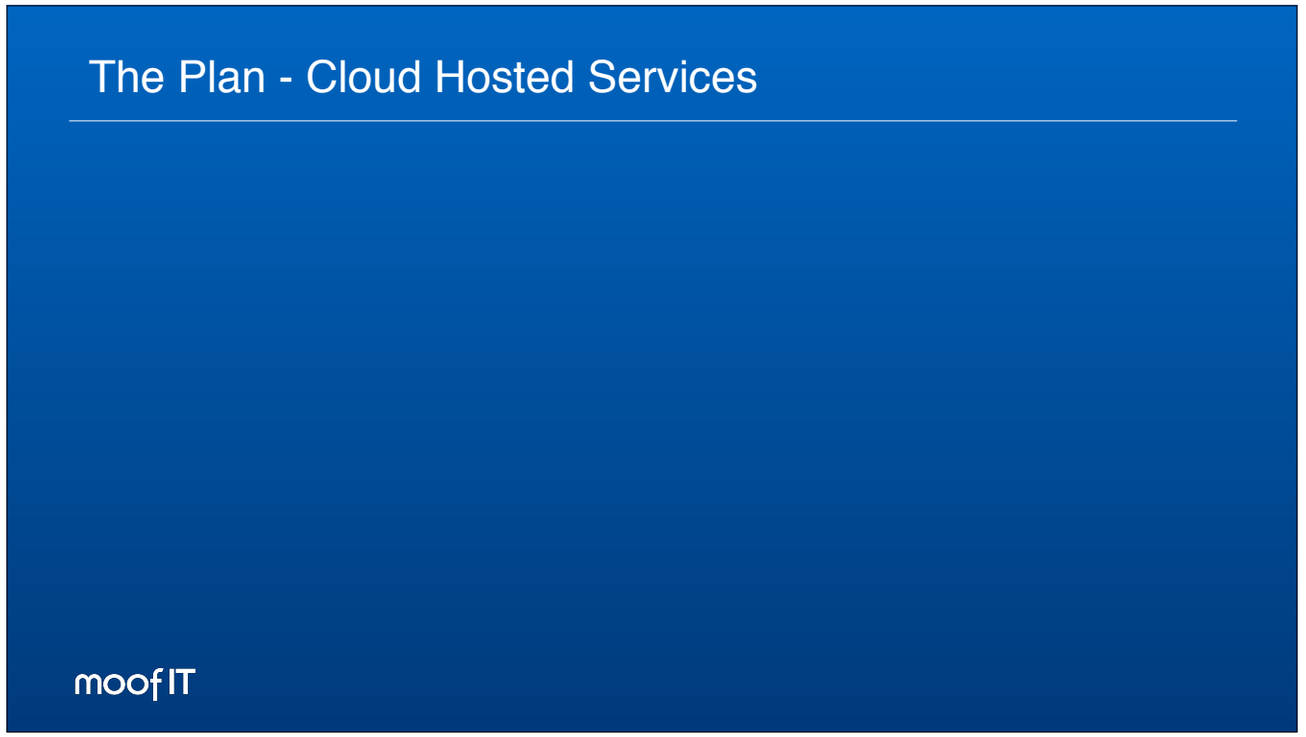


For the end devices we didn't want to completely lock down users. After-all, they're adults and employees, so we were not gonna to treat them as kids at school. In this spirit we were only looking to enforce what we felt was the minimum requirements to meet the baselines.
So the plan as far as the client devices go included:
CLICK
- Enrolment in a management solution
    - As a Jamf Partner and Integrator, we opted to use Jamf Pro as the solution here.

CLICK
- Full Disk encryption on all laptops
    - FileVault for this. As it's built into the OS, it was both the cheapest, and the least likely to have issues, especially with things like OS updates.

CLICK
- Password policies on devices:
    - As per the more recent advice from 'National Institute of Standards and Technology' (NIST), we're staying away from maximum password ages - aka "Change your password every 90 days"

CLICK
- Software patch policies with deadlines
    - Applications and OS updates



For the cloud-based services, we wanted to do as much as we can as they'll be public facing by their nature

CLICK

- Password policies where possible:
    - Again, pretty much the same as for end devices

CLICK

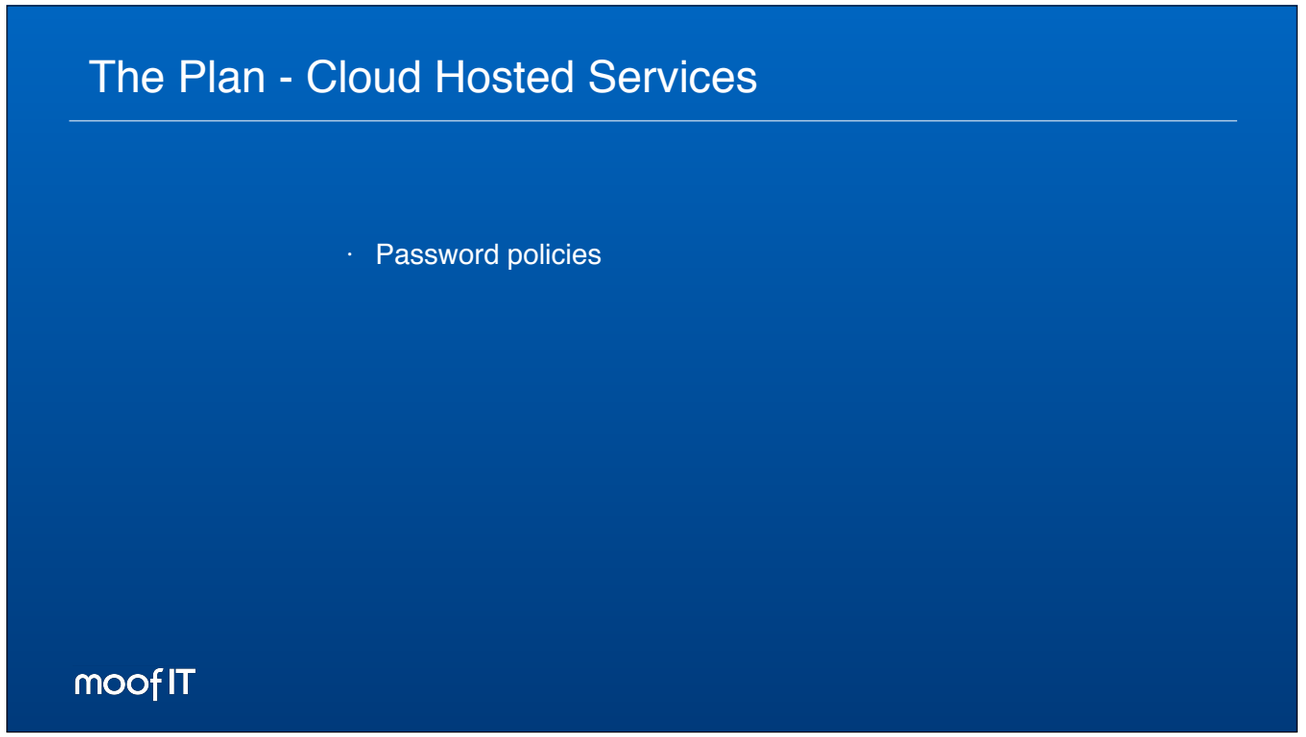
- Multi-Factor Authentication on all services that can take it
    - Ideally App-based, falling back to SMS if there's no other option

CLICK

- Requiring the use of non-shared accounts
    - To be able to track who does what, to control (including revoke) access should someone leave, and to comply with regulations as best as we can.

CLICK

- Changing administration passwords
    - As these had been used by various employees previously, these were all changed with the Technical Director with only that person having access



For the cloud-based services, we wanted to do as much as we can as they'll be public facing by their nature

CLICK

- Password policies where possible:
    - Again, pretty much the same as for end devices

CLICK

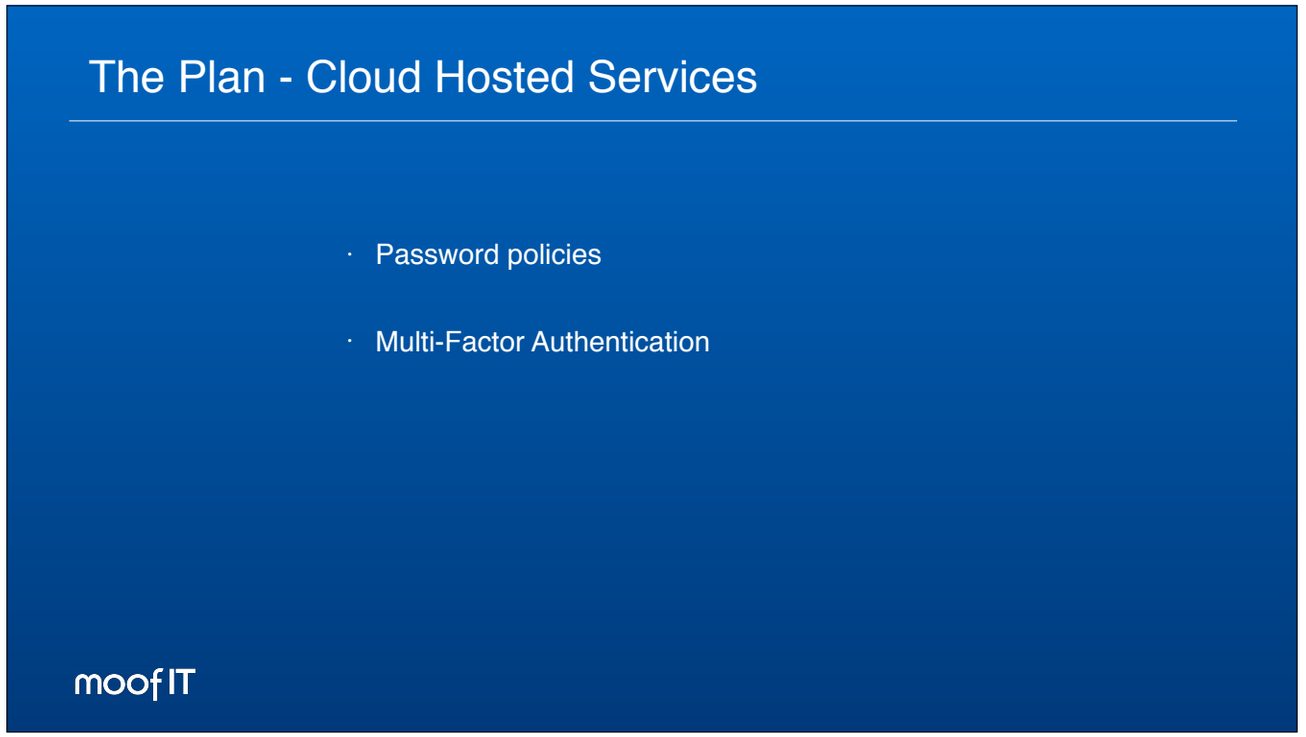
- Multi-Factor Authentication on all services that can take it
    - Ideally App-based, falling back to SMS if there's no other option

CLICK

- Requiring the use of non-shared accounts
    - To be able to track who does what, to control (including revoke) access should someone leave, and to comply with regulations as best as we can.

CLICK

- Changing administration passwords
    - As these had been used by various employees previously, these were all changed with the Technical Director with only that person having access

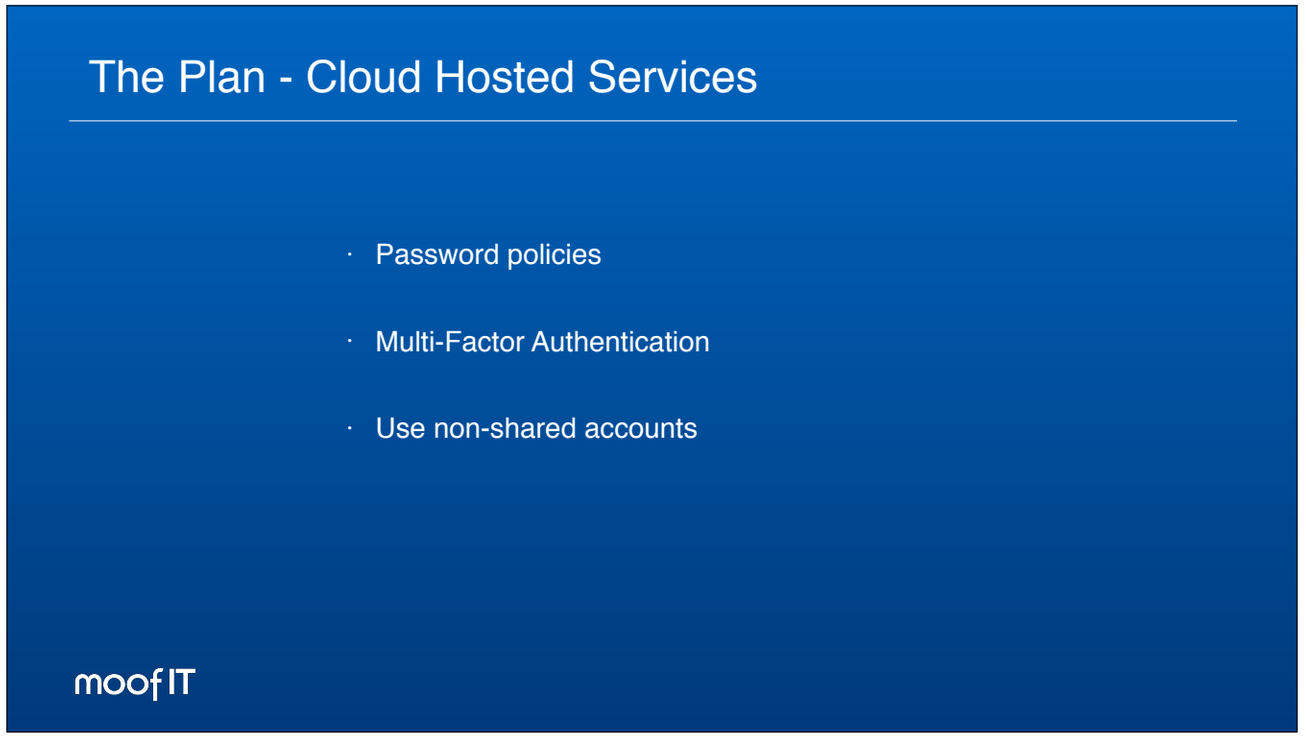


For the cloud-based services, we wanted to do as much as we can as they'll be public facing by their nature
CLICK
- Password policies where possible:
    - Again, pretty much the same as for end devices

CLICK
- Multi-Factor Authentication on all services that can take it
    - Ideally App-based, falling back to SMS if there's no other option

CLICK
- Requiring the use of non-shared accounts
    - To be able to track who does what, to control (including revoke) access should someone leave, and to comply with regulations as best as we can.

CLICK
- Changing administration passwords
    - As these had been used by various employees previously, these were all changed with the Technical Director with only that person having access



For the cloud-based services, we wanted to do as much as we can as they'll be public facing by their nature

CLICK

- Password policies where possible:
    - Again, pretty much the same as for end devices

CLICK

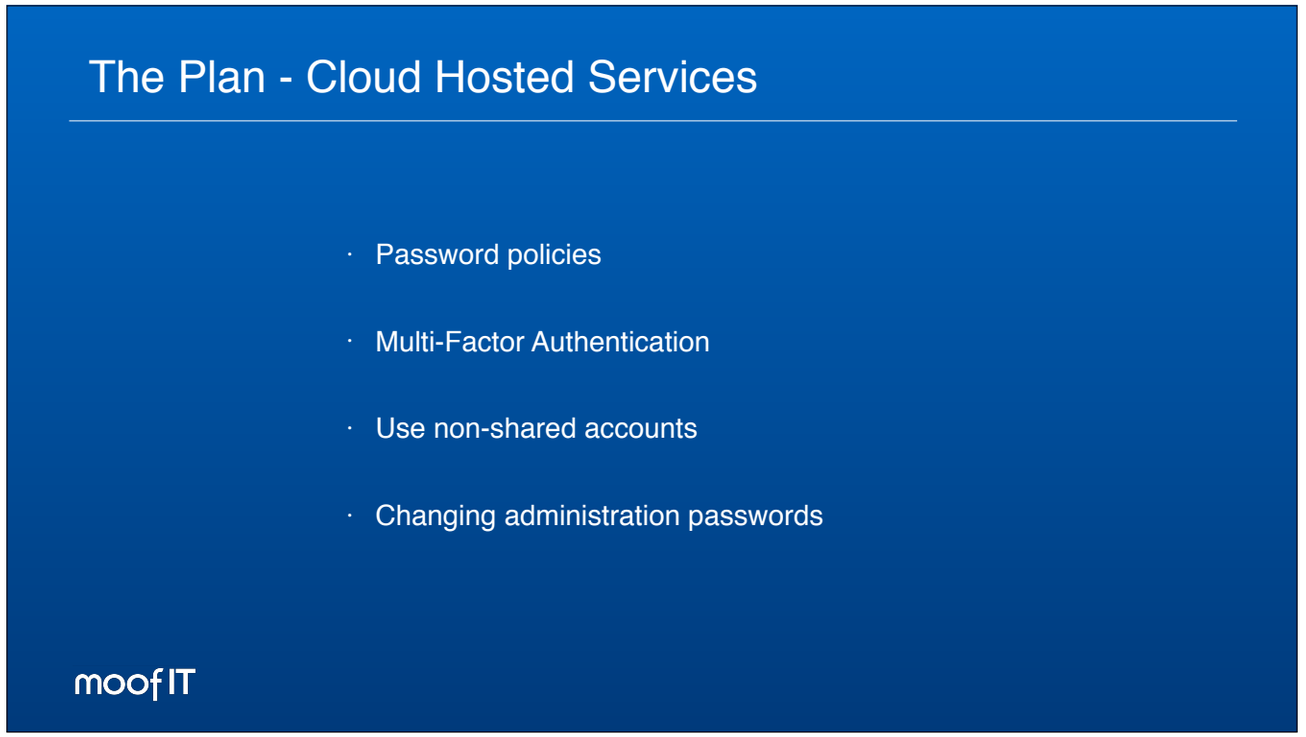
- Multi-Factor Authentication on all services that can take it
    - Ideally App-based, falling back to SMS if there's no other option

CLICK

- Requiring the use of non-shared accounts
    - To be able to track who does what, to control (including revoke) access should someone leave, and to comply with regulations as best as we can.

CLICK

- Changing administration passwords
    - As these had been used by various employees previously, these were all changed with the Technical Director with only that person having access



For the cloud-based services, we wanted to do as much as we can as they'll be public facing by their nature

CLICK

- Password policies where possible:
    - Again, pretty much the same as for end devices

CLICK

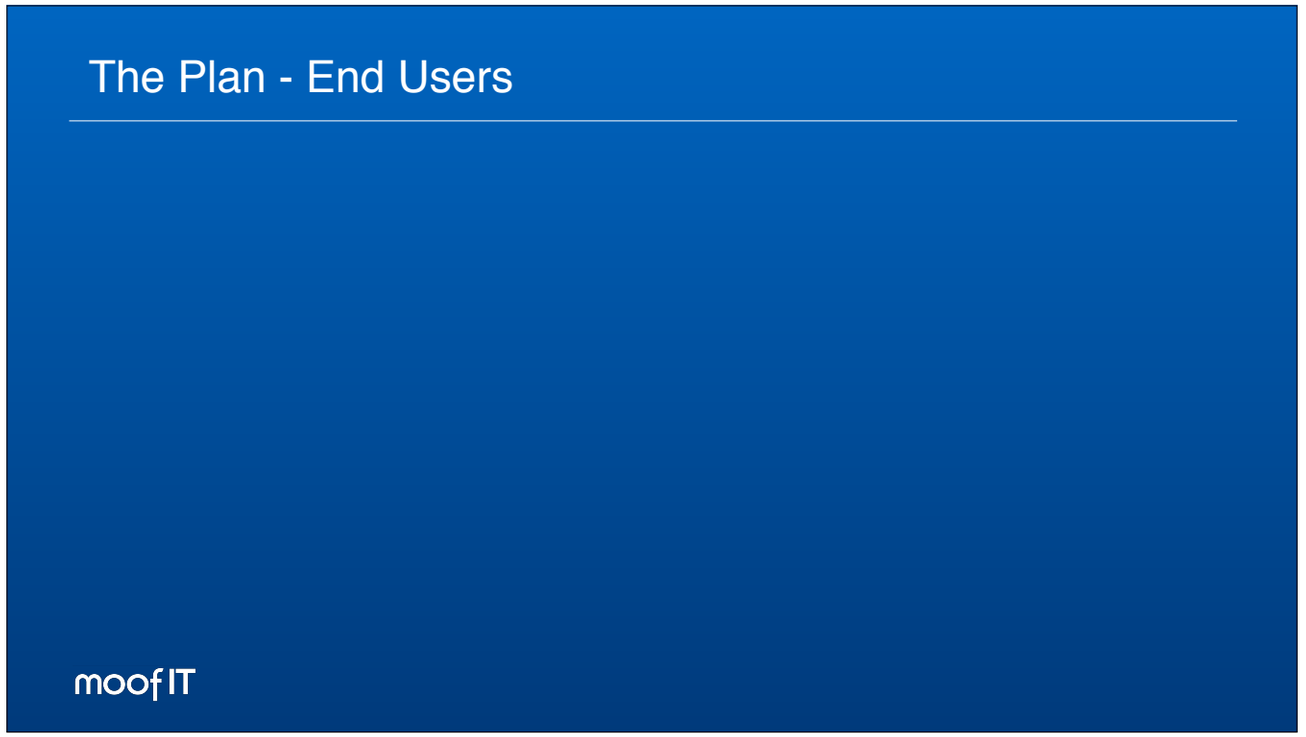
- Multi-Factor Authentication on all services that can take it
    - Ideally App-based, falling back to SMS if there's no other option

CLICK

- Requiring the use of non-shared accounts
    - To be able to track who does what, to control (including revoke) access should someone leave, and to comply with regulations as best as we can.

CLICK

- Changing administration passwords
    - As these had been used by various employees previously, these were all changed with the Technical Director with only that person having access



And for the end users:

CLICK

- Write, shared and discussed an official company IT security policy document.
    - Including required points, suggested / recommend points and fair non-work usage details
    - This also included what items would be enforced via management solutions, and which would be expected of the employee

CLICK

- Discussions around password usage
    - Including advice around password re-use, and possible password managers

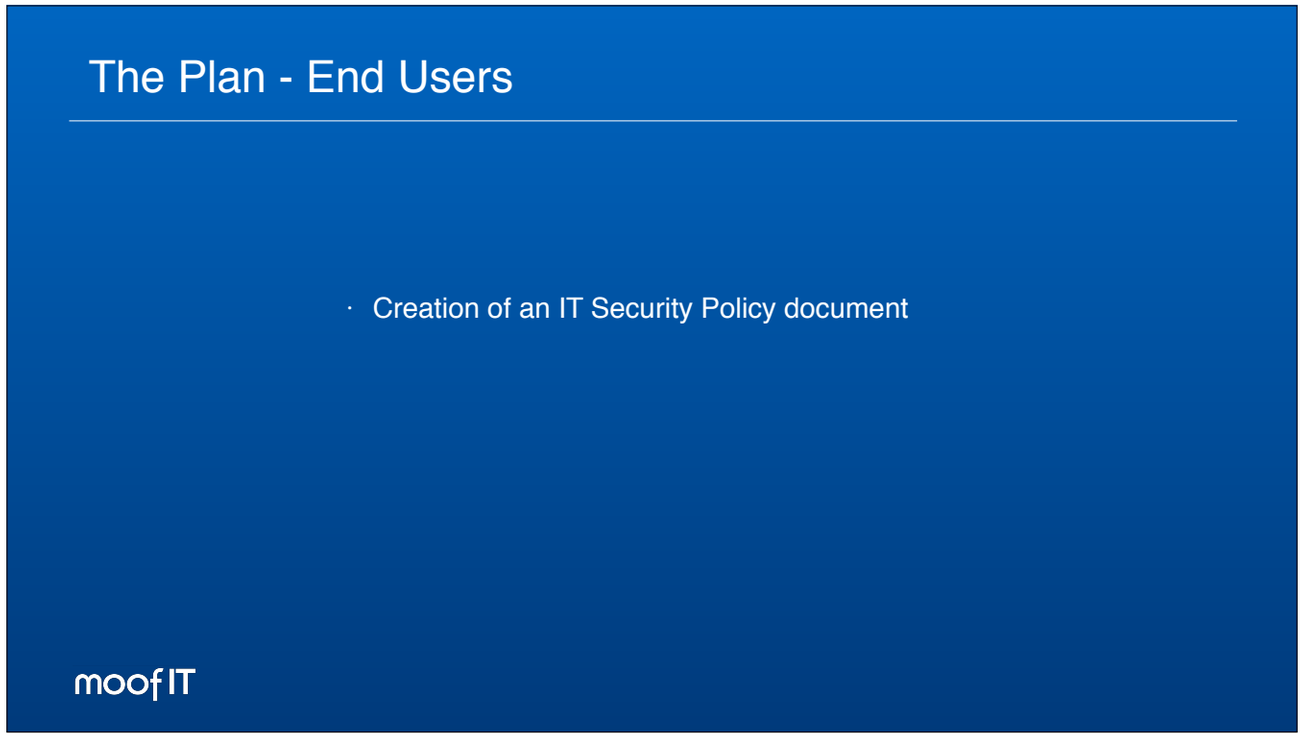
CLICK

- Documentation!
    - Documentation would be created for everything that may affect them as part of the project (such as Multi-Factor authentication, FileVault, password policies etc).
    - This would be emailed to staff members, made available on internal HR systems and discussed in-person.

CLICK

- Rollout
    - The changes were planned to be staggered department by department, over the course of a few months. This would proivide a chance for staff to opt into the change before it became compulsory, and to provide feedback

Right, We've got own goals sorted, and our plan. How'd it go?



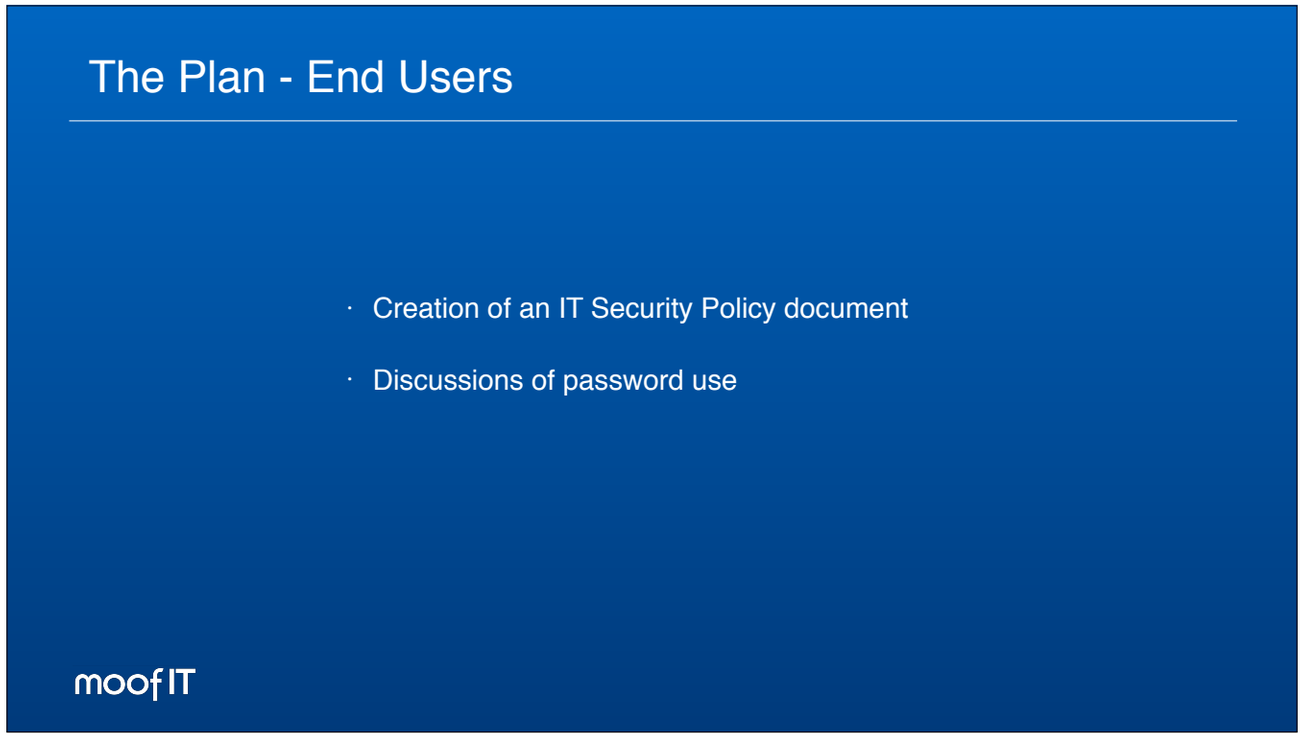
And for the end users:
CLICK
- Write, shared and discussed an official company IT security policy document.
    - Including required points, suggested / recommend points and fair non-work usage details
    - This also included what items would be enforced via management solutions, and which would be expected of the employee

CLICK
- Discussions around password usage
    - Including advice around password re-use, and possible password managers

CLICK
- Documentation!
    - Documentation would be created for everything that may affect them as part of the project (such as Multi-Factor authentication, FileVault, password policies etc).
    - This would be emailed to staff members, made available on internal HR systems and discussed in-person.

CLICK
- Rollout
    - The changes were planned to be staggered department by department, over the course of a few months. This would proivide a chance for staff to opt into the change before it became compulsory, and to provide feedback

Right, We've got own goals sorted, and our plan. How'd it go?



And for the end users:

CLICK

- Write, shared and discussed an official company IT security policy document.
    - Including required points, suggested / recommend points and fair non-work usage details
    - This also included what items would be enforced via management solutions, and which would be expected of the employee

CLICK

- Discussions around password usage
    - Including advice around password re-use, and possible password managers

CLICK

- Documentation!
    - Documentation would be created for everything that may affect them as part of the project (such as Multi-Factor authentication, FileVault, password policies etc).
    - This would be emailed to staff members, made available on internal HR systems and discussed in-person.

CLICK

- Rollout
    - The changes were planned to be staggered department by department, over the course of a few months. This would proivide a chance for staff to opt into the change before it became compulsory, and to provide feedback

Right, We've got own goals sorted, and our plan. How'd it go?

And for the end users:

CLICK

- Write, shared and discussed an official company IT security policy document.
    - Including required points, suggested / recommend points and fair non-work usage details
    - This also included what items would be enforced via management solutions, and which would be expected of the employee

CLICK

- Discussions around password usage
    - Including advice around password re-use, and possible password managers

CLICK

- Documentation!
    - Documentation would be created for everything that may affect them as part of the project (such as Multi-Factor authentication, FileVault, password policies etc).
    - This would be emailed to staff members, made available on internal HR systems and discussed in-person.

CLICK

- Rollout
    - The changes were planned to be staggered department by department, over the course of a few months. This would proivide a chance for staff to opt into the change before it became compulsory, and to provide feedback

Right, We've got own goals sorted, and our plan. How'd it go?

And for the end users:
CLICK
- Write, shared and discussed an official company IT security policy document.
    - Including required points, suggested / recommend points and fair non-work usage details
    - This also included what items would be enforced via management solutions, and which would be expected of the employee

CLICK
- Discussions around password usage
    - Including advice around password re-use, and possible password managers

CLICK
- Documentation!
    - Documentation would be created for everything that may affect them as part of the project (such as Multi-Factor authentication, FileVault, password policies etc).
    - This would be emailed to staff members, made available on internal HR systems and discussed in-person.

CLICK
- Rollout
    - The changes were planned to be staggered department by department, over the course of a few months. This would proivide a chance for staff to opt into the change before it became compulsory, and to provide feedback

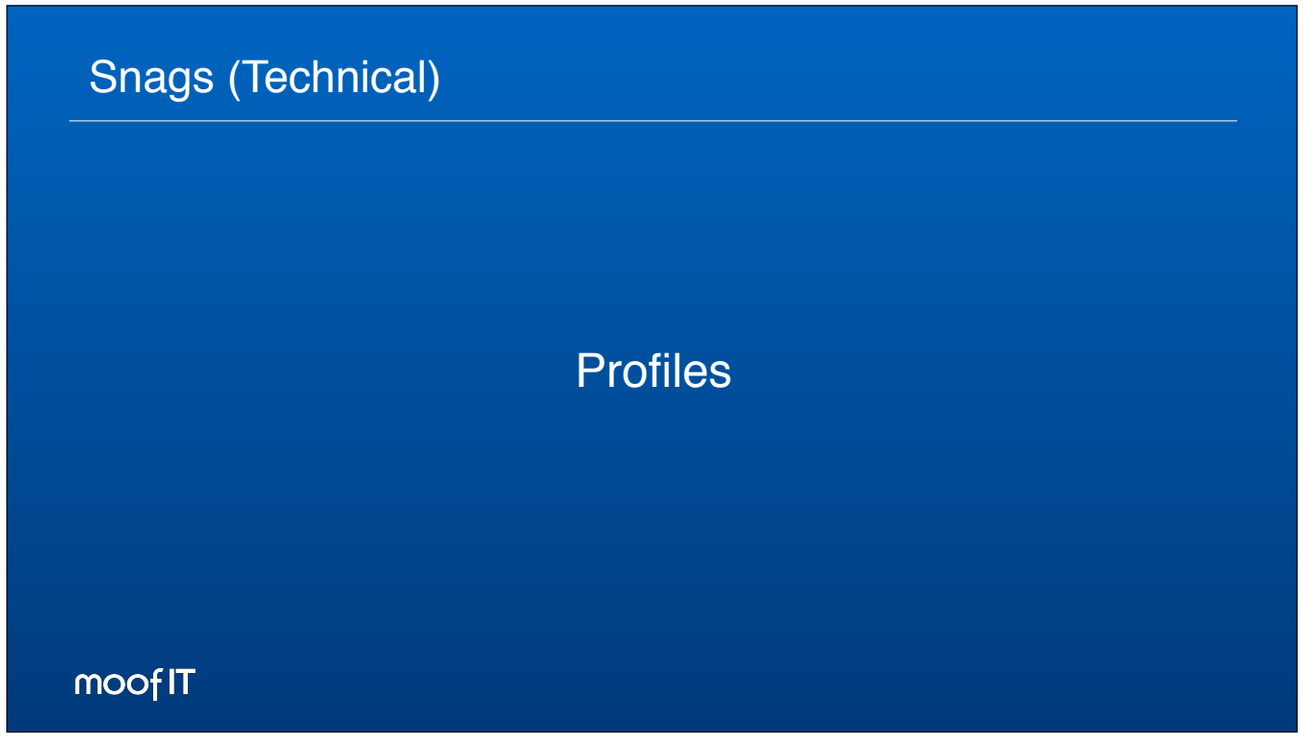
Right, We've got own goals sorted, and our plan. How'd it go?

Snags (Technical)

So, what snags did I hit?

Snags (Technical)

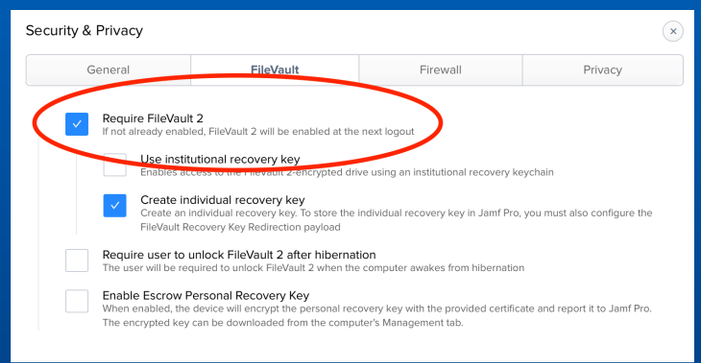
So, what snags did I hit?



The first snag we hit was with configuration profiles and their lack of surgical-ness.

One of the biggest issues we had, is that if you wish to only set a single item in a specific payload section, you must set all the items in all the tabs, within that payload

Snags (Technical) - Profiles

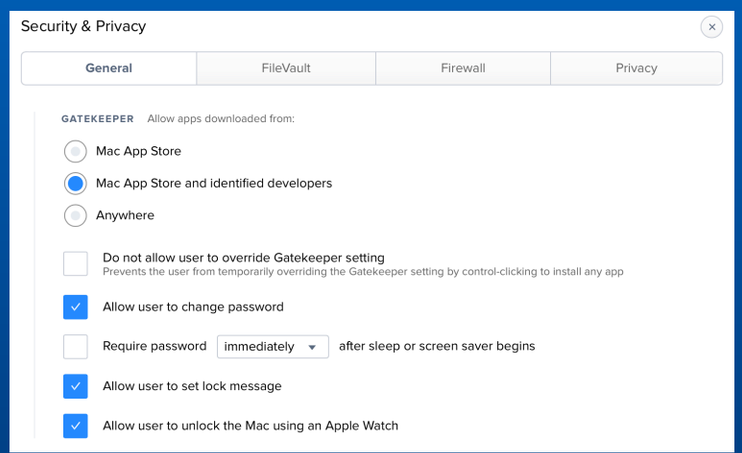


moof IT

For example, we wanted to set a requirement for FileVault under "Security & Privacy", as shown here.

However, it will also set (and enforced) all settings in the other three tabs, including...

Snags (Technical) - Profiles



moof IT

(by default)

- Disabling the password after screen-saver requirement

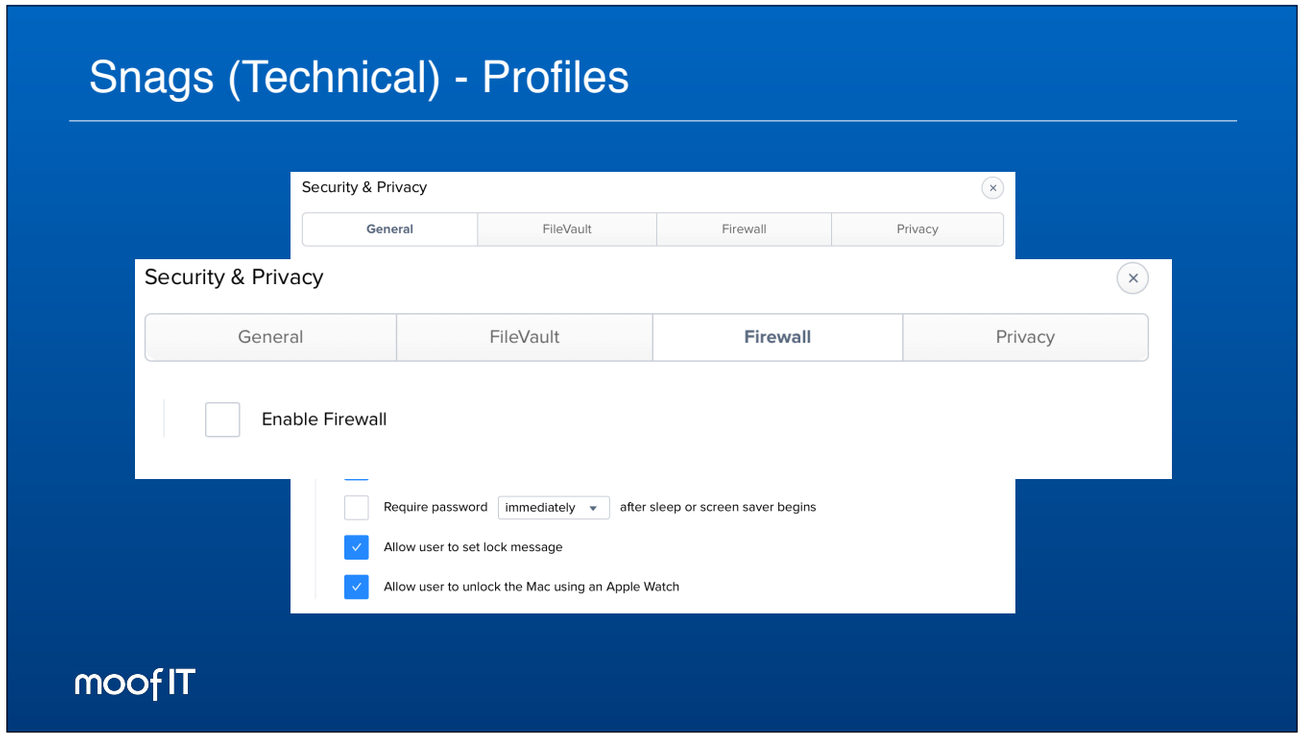
Click

- Disabling the Firewall

Click

- Allowing sending usage data

My solution was to build a custom configuration profile for this.



(by default)

- Disabling the password after screen-saver requirement

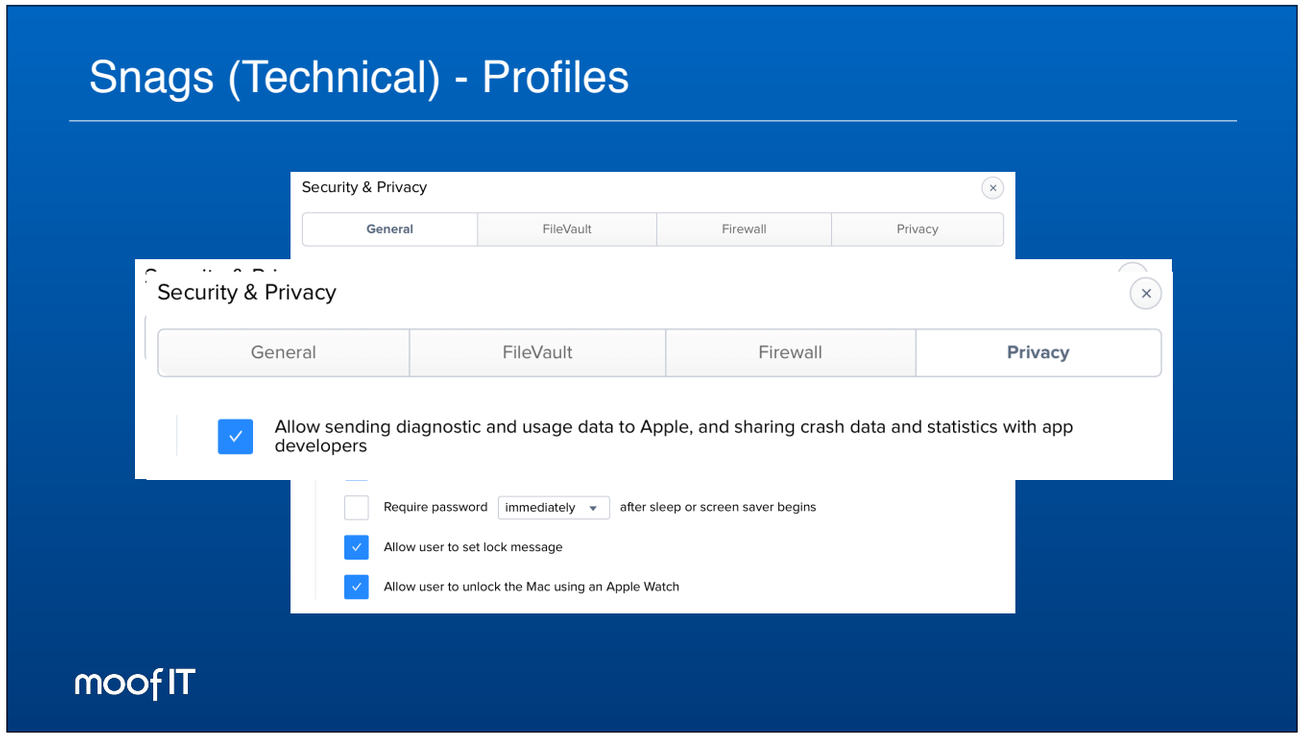
Click

- Disabling the Firewall

Click

- Allowing sending usage data

My solution was to build a custom configuration profile for this.



(by default)

- Disabling the password after screen-saver requirement

Click

- Disabling the Firewall

Click

- Allowing sending usage data

My solution was to build a custom configuration profile for this.

Snags (Technical) - Profiles

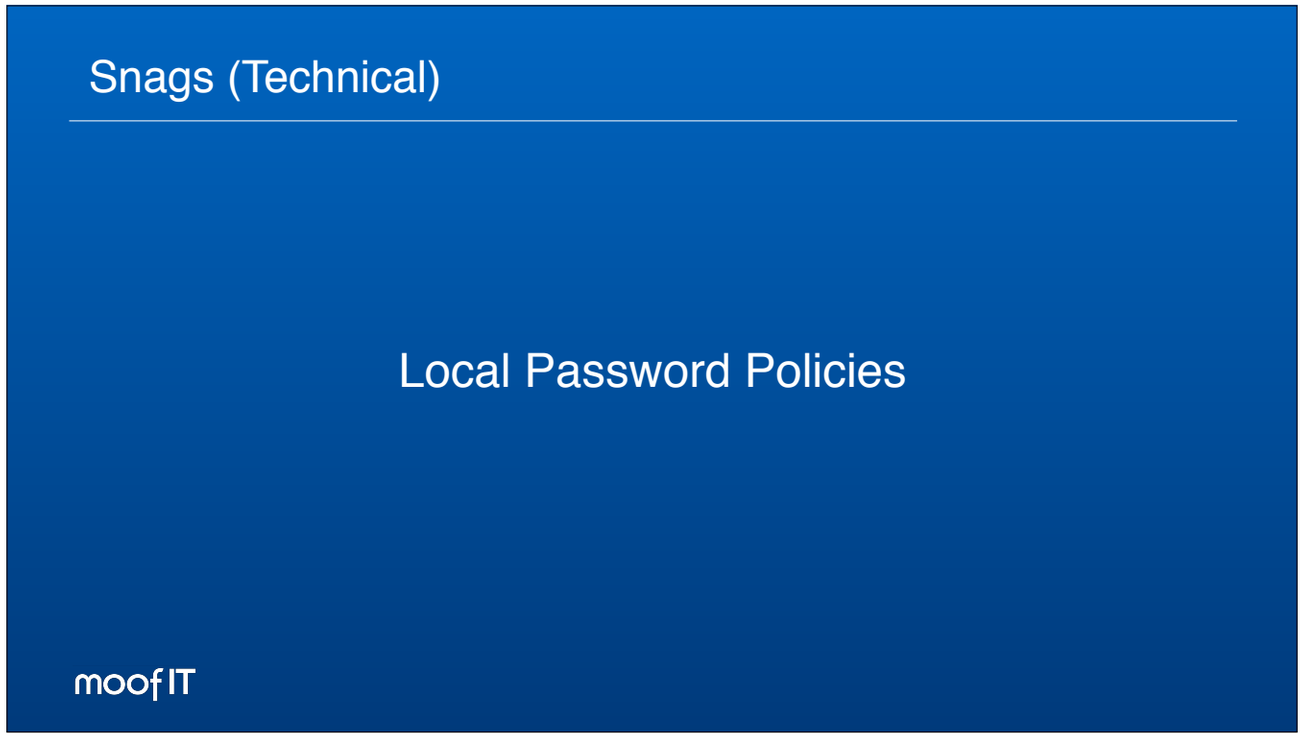
http://www.amsys.co.uk/2017/08/profile-enable-filevault-2/

https://youtu.be/nKgOWvC6p64?t=13m12s

moof IT

I've detailed the profile I ended up building in this blog post (pre-10.13 only)
This also isn't just Jamf. Other 3rd Party MDM providers, and Apple's own Reference solution, Profile Manager, has the same issue
Eric Gomez has also discussed this more in a presentation he delivered at Macbrained, San Francisco, also linked above (around 13 minutes in).

Just a reminder that all links will be in a follow up blog post, so don't necessarily worry about jotting this down now.

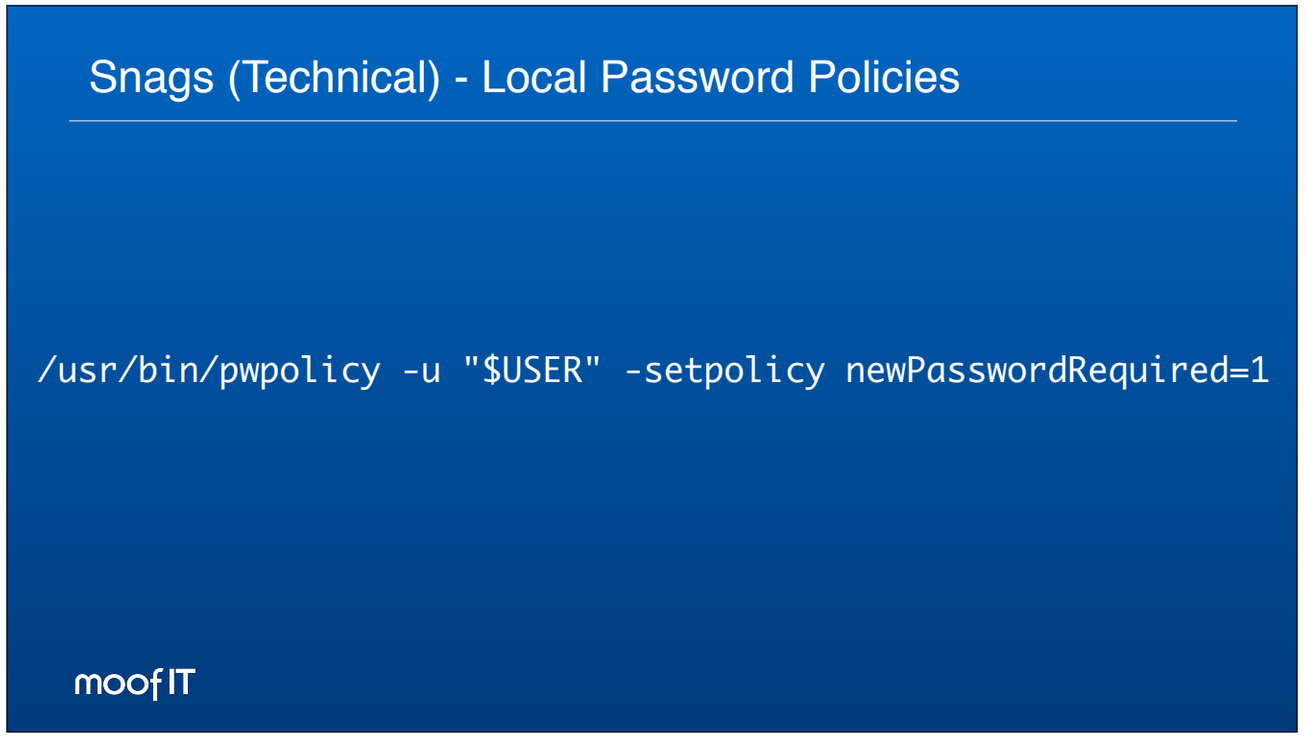


The second snag I hit was with local password policies on macOS.

If you deploy a password policy to a macOS device (in my case, using the 'passcode' profile payload), that policy won't check against existing passwords.

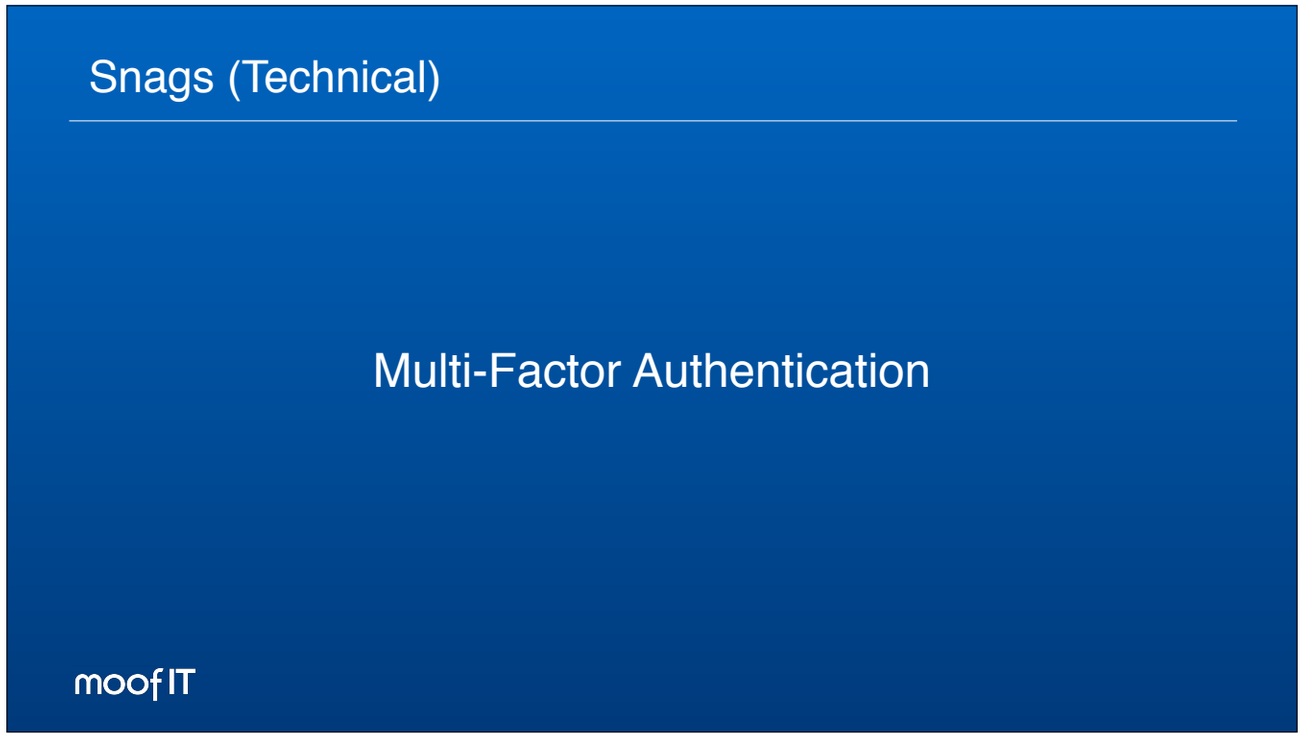
In hindsight, it's a little obvious as it would mean the OS would have to store all password in a reversal-able format, which isn't ideal!

However, we had to make sure that user's passwords were meeting these new requirements.



Turns out I wasn't the only one who has this issue. it's come up a fair bit across the Mac Admin community over the years.
The 'solution' is to expire the user's account password, to force a 'new' password to be set at next login, using the above command.
Thanks to Graham Gilbert, who confirmed this with me over Slack, just to make sure I wasn't missing anything obvious.

Another tip is, if you **don't** set a Password History requirement, and the user's previous password already meets the requirements set in the policy, the user can use their existing password again.



The next snag I hit was around multi-factor authentication.
This boils down to a number of whinges if I'm honest but:

- Some cloud services do not offer any Multi-Factor authentication
- Some offer Multi-Factor Authentication, but it's not an enforceable requirement by, say, an administrator
- Others only offer that option if you opt for higher-costing tiers of their service
- And finally, some are just bizarre:

More than one provider required the administrator to actually perform the multi-factor setup for the user, i.e. the user couldn't set it up themselves, and when you click to enable it, the admin console simply displayed the user's QR code and confirmation form.

Snags (Technical)

Patching of devices

moof IT

Last snag worth mentioning is patching of devices.

- As an IT support company, we need to ensure our clients are as protected as possible.
- However, as an external entity, tying user's devices up at inconvenient times can kill a business relationship.
- This same concern applies to internal IT support and your users.

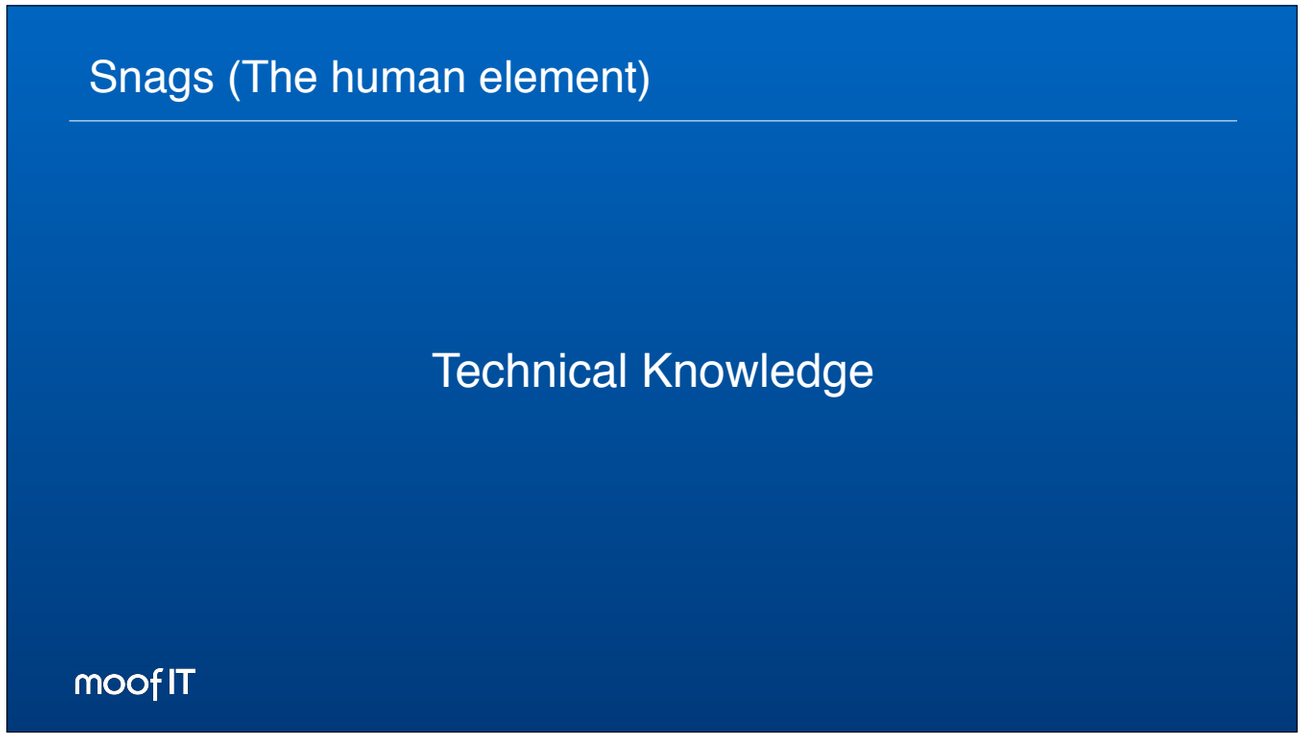
We're still testing various options for this, including enforcing an immediate patching run if user's fail to 'opt-in' to be patched within a set time period, to reporting them to our primary contacts onsite.

Snags (The ~~fifth~~ human element)

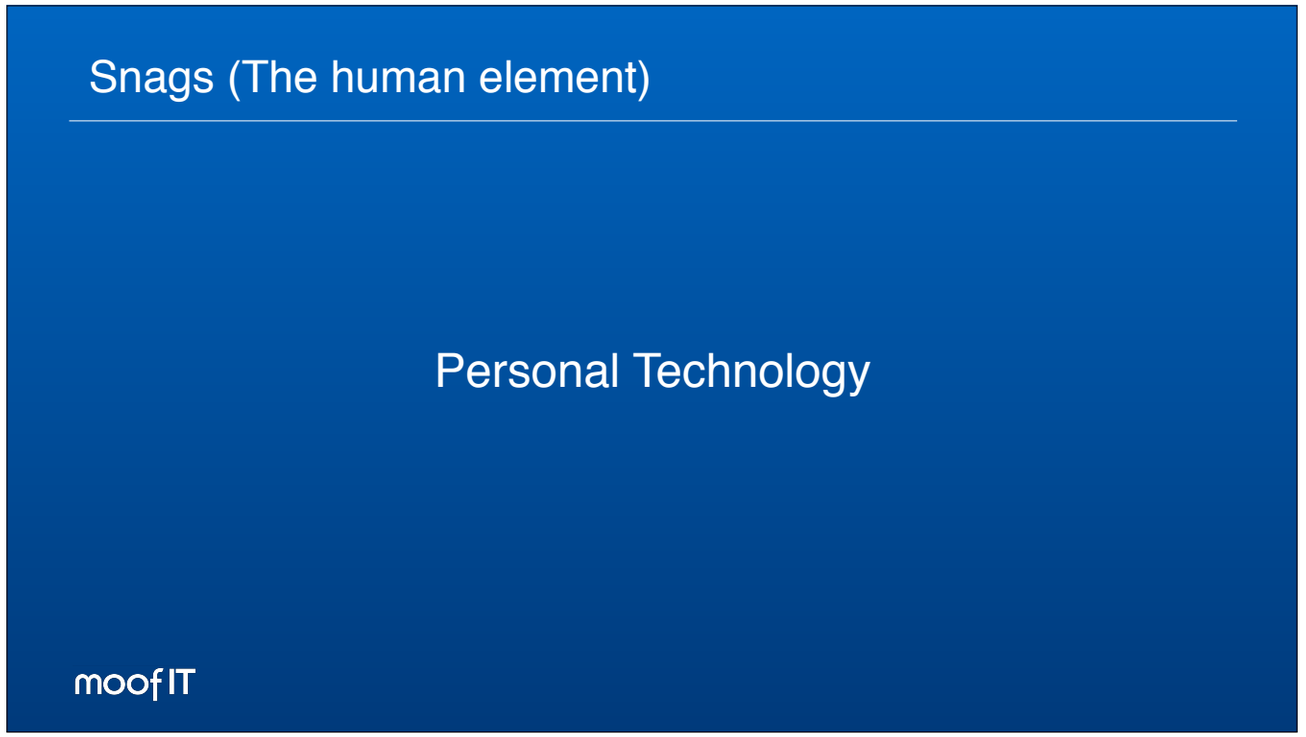
What about the other snags? The human side of things?

Snags (The ~~fifth~~ human element)

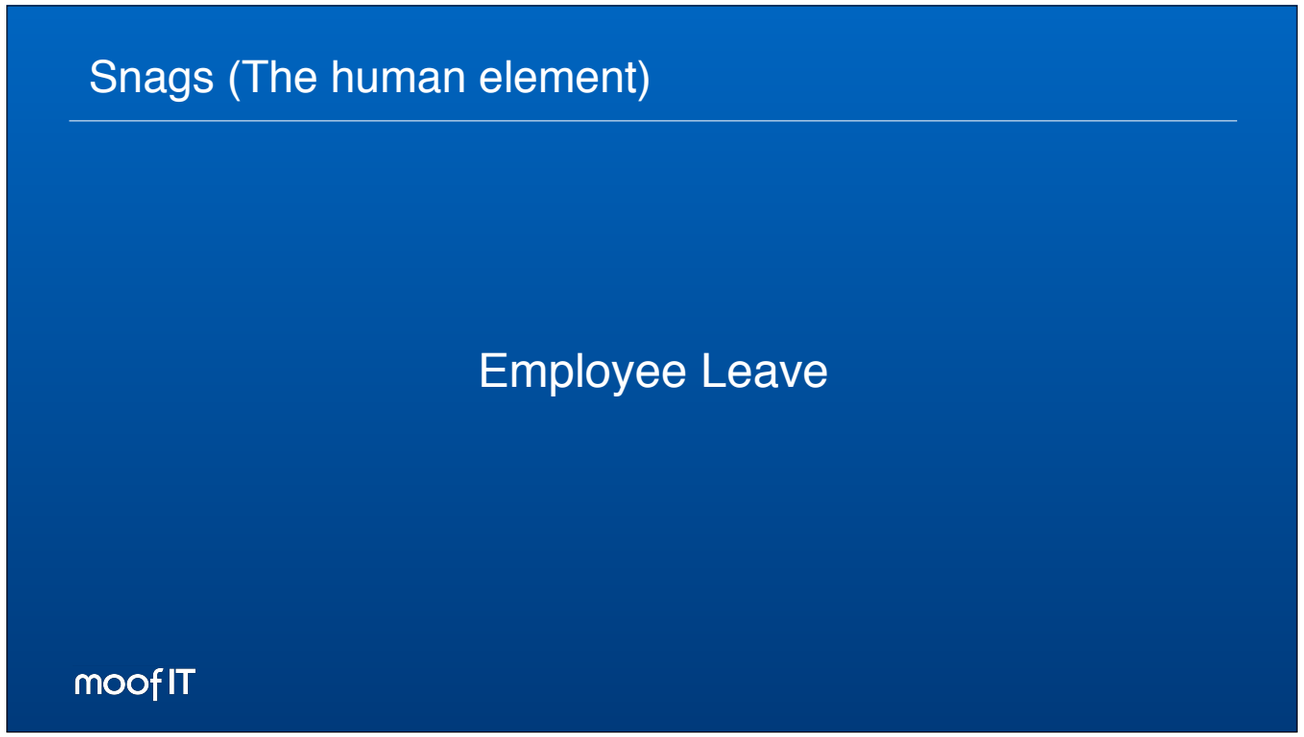
What about the other snags? The human side of things?



One thing we under-estimated was the technical knowledge of the employees.
Like all of us here, living and breathing tech 40 hours a week (or more), it's very, very easy to forget the typical levels of knowledge of the average user.
Some might have no idea what Multi-Factor Authentication is, let alone how it will affect their work life with these changes.
Again, this isn't something that should be blamed on the users. Put me in front of Sage or Photoshop and I'd be hopeless!



So one of the big tasks of this project was to roll out Multi-Factor authentication to as many services as possible.
One unforeseen snag, especially in this day and age, is not every user is guaranteed to have a smart phone!
Huh, right?
This company also didn't supply users with devices, so for this instance, we set the user up with SMS based Multi-Factor (better than none), and the company were to provide that user with a work device specifically for that purpose.



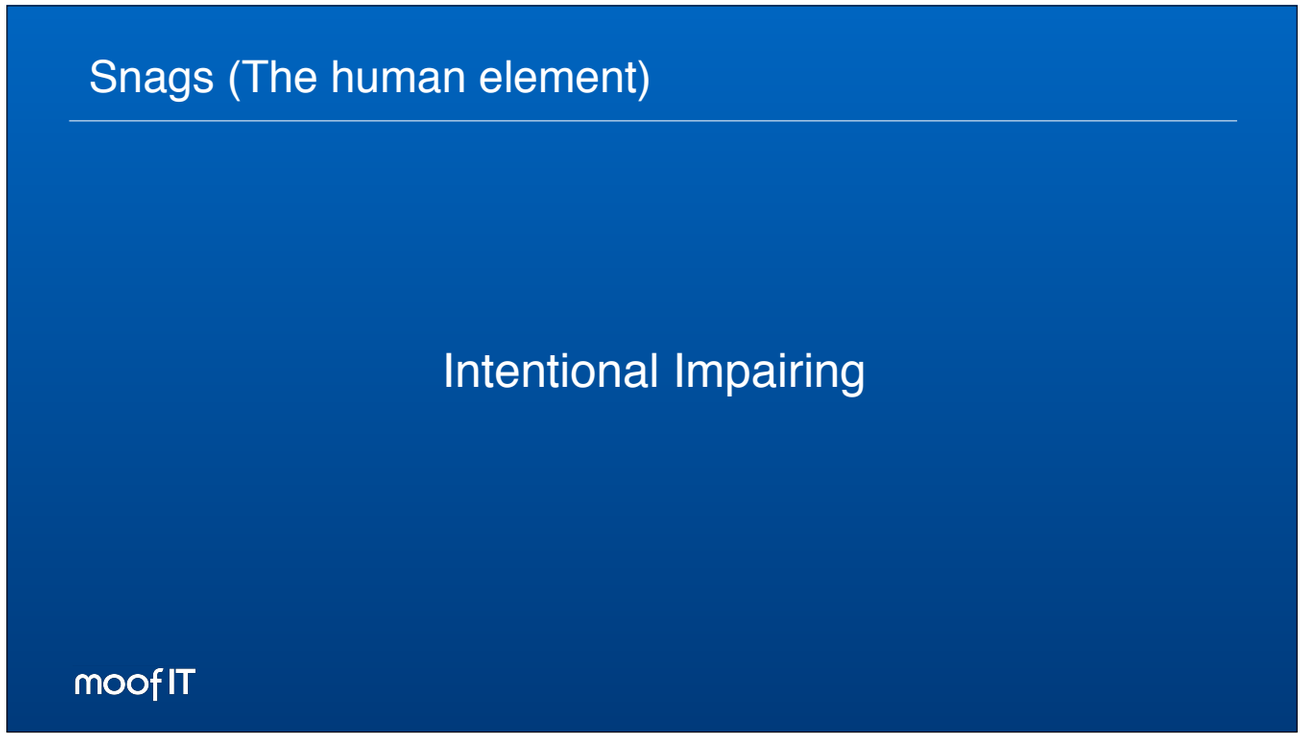
Something else you may not consider when your working hard to solve technical challenges is, will the right users be available before the rollout deadlines?
Over the course of this project, we had a few people on long-term sick leave, others on maternity / paternity leave, and one who was off on a 4 week honeymoon.
Although it didn't cause that large of an issue to the rollouts, it was something easily overlooked when concentrating on the technical side.

Snags (The human element)

Documentation

moof IT

In some cases the documentation wasn't read, or fully understood.
Being a technical person, who's created tons of documentation for other technical people, makes this a very easy trap to fall into.
In various places, the documentation used too much unnecessary technical language, was too long or didn't have enough screenshots.



And in some cases, we did have intentionally disruptive snags. This included:

- Refusing to read the documentation at all
- Passive aggressive refusal, like ignoring emails requesting action be taken, or feedback provided
- Push back on the last day of a rollout deadline, often after combinations of the above.

Being an external company, we had to tread carefully in these instances, including moving deadlines, making temporary exceptions, and ensuring that any deadlines and messages are sent via writing (email in this case).

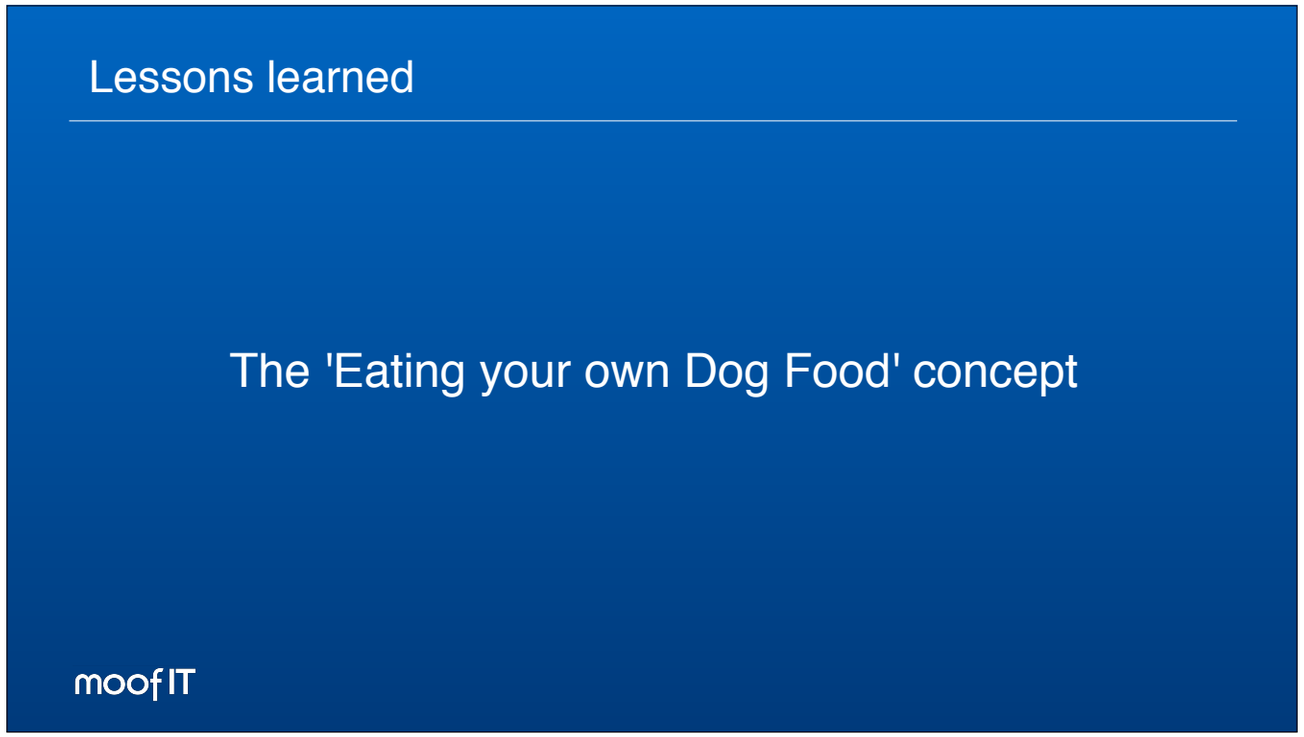
But the bottom line is we had full backing of the company's directors and that was always an ace in the hole. Thankfully we didn't have to play, or threaten to play, that card (which is the ideal way to carry this out).

Lessons learned (aka tips and tricks)

So, after all that, what do we learn? What advice or tips can we pass on?

Lessons learned (aka tips and tricks)

So, after all that, what do we learn? What advice or tips can we pass on?



The Dog Food concept.
If you're rolling these changes out to your own organisation, you (and possibly your team) should be the first to have the changes. You should also continuing using the system with the changes you expect users to use.
If you can't do your job then it's likely your users can't either.
If you're rolling this out to another company, not only should you try to run them yourself, the client's management teams should also be using them, if they expect their team members to do so.

Lessons learned

Documentation

moof IT

Documentation should be written for the intended audience, not the author.
If your documentation is aimed at end users, write it for end users.
If the process is complicated consider, adding in screenshots with annotations, and detailed step-by-step instructions.
If the documentation is long, consider how it could be broken up. Either into sections or even different documents.
If the documentation is not confidential, why not try it on other members of your team, or even family?
I've tested generic end user guides on random family members to see if it holds up.

Lessons learned

Staggered Rollouts

moof IT

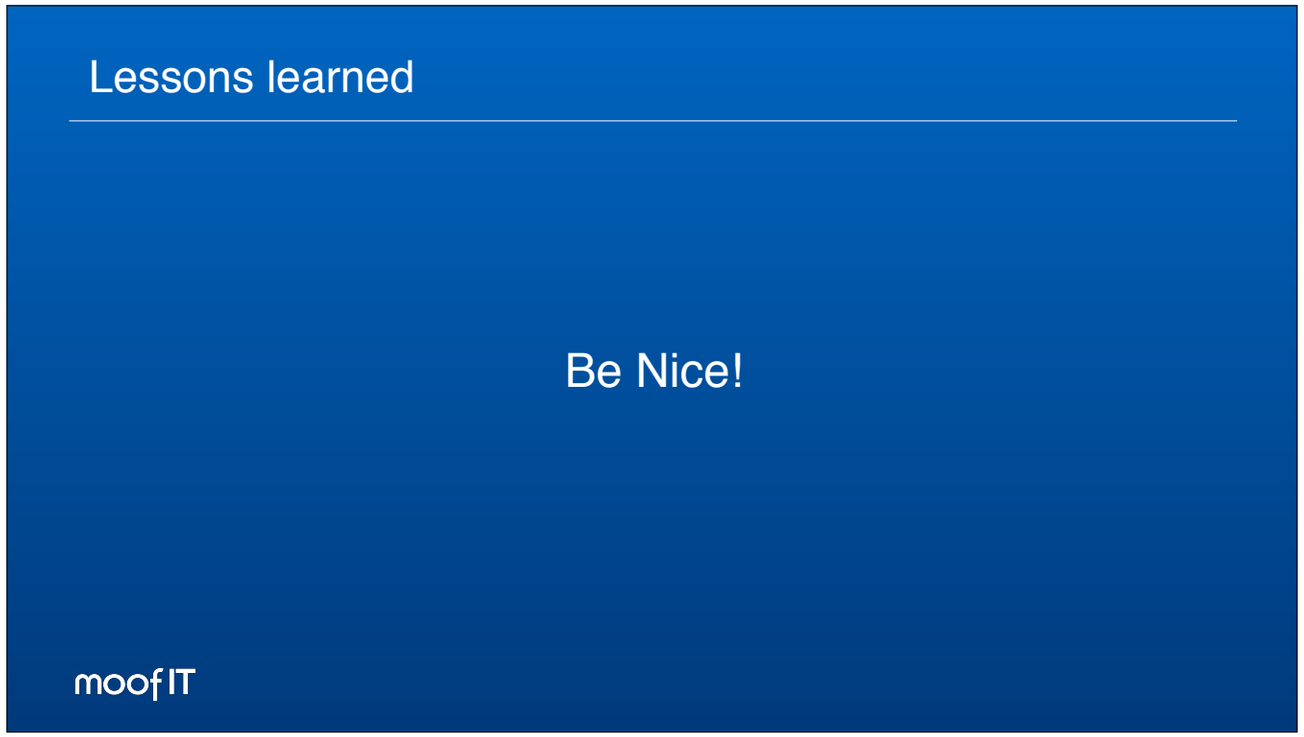
Stage and test rolling out changes. Not just to test the technical side, but to test how it will go down with users.
Ideally, you should try to test with the most and least technical person in each area where possible.
This will also serve to test your documentation of these changes, allowing you to amend those docs prior to full rollouts.
aka Fine-tuning

Lessons learned

Get appropriate support and approval

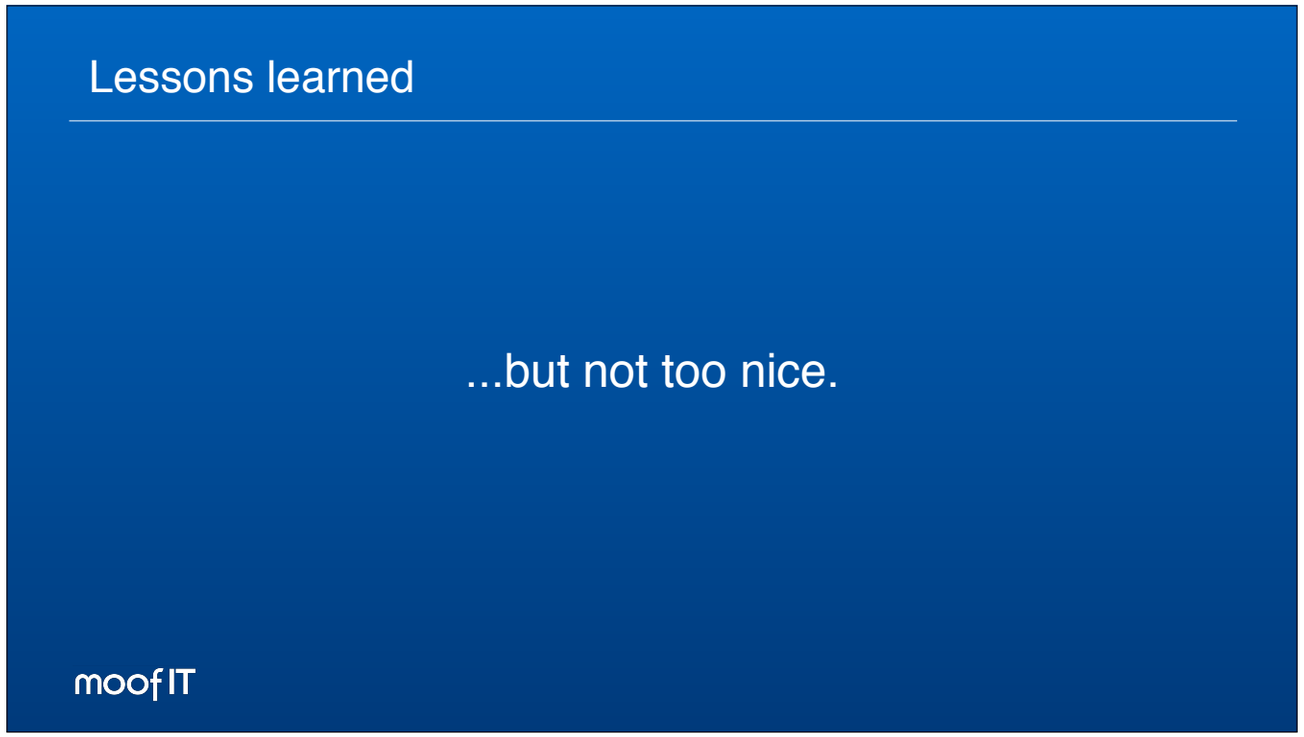
moof IT

Make sure you have the right backing for changes.
For example, we made sure we had full support from the Directors of the company before rolling out the changes in this project. We also made sure to notify them of various deadlines and timeframes, as well as the changes and risks with each change and not carrying them out.
This allowed us to push certain aspects harder when changes were resisted or ignored.

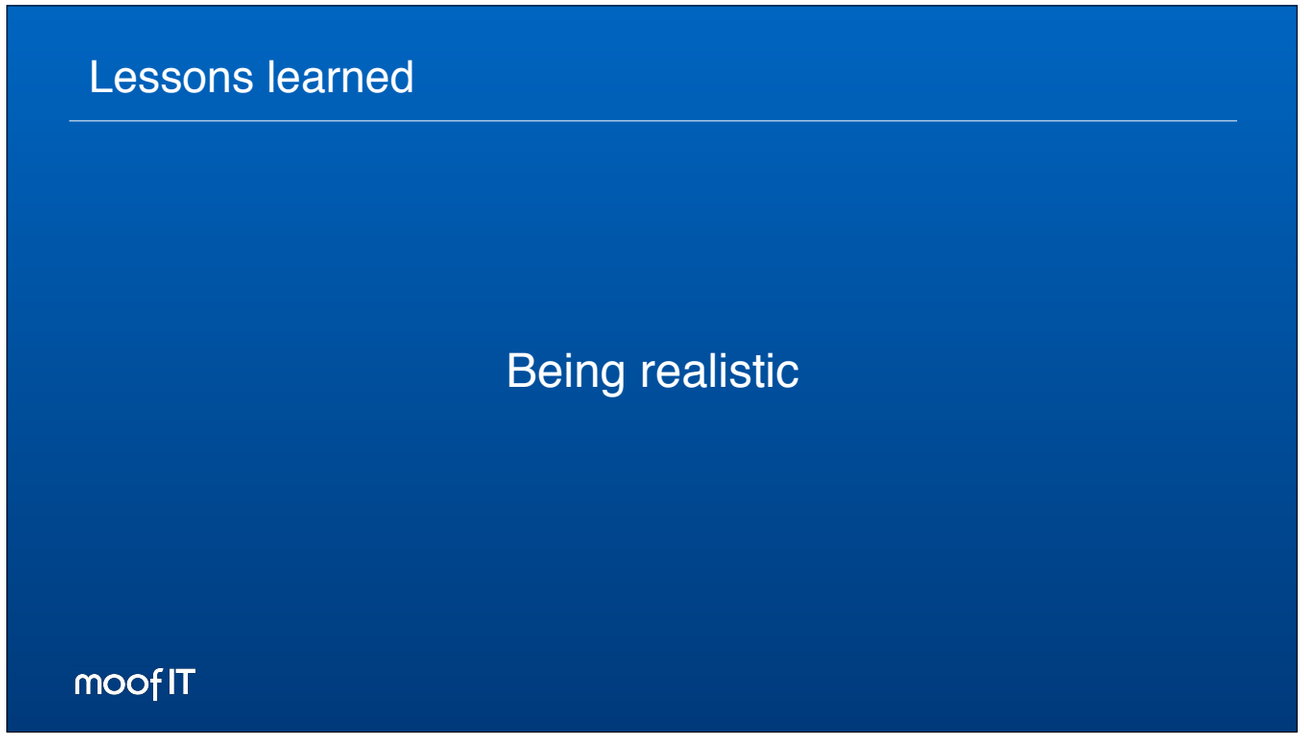


Some changes will be highly disruptive and will affect the work output of the users. Be understanding of this, and try to be as flexible as possible.

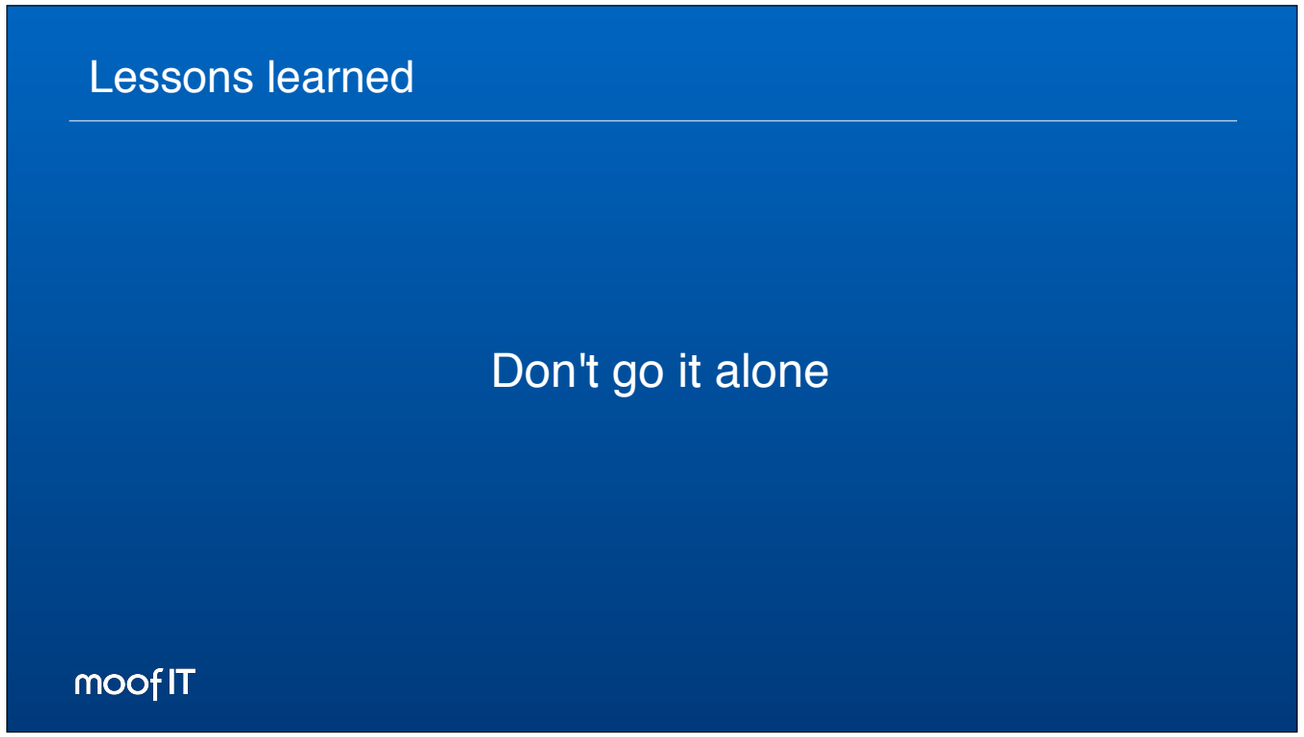
Imagine If I locked down Slack on your Mac? I don't know about you all, but that'd affect my work-output a lot (either way is arguable!) but it'd also annoy me considerably.



You will sometimes encounter users and even senior staff who will push back (either intentional or not). Sometimes you will need to push ahead with the changes.
For example, in the earlier phases we requested volunteers to test new changes for their areas of the business. After pushing back the deadlines a few times due to lack of volunteers, we sent out a final deadline communication, then pushed the changes (with full approval of the relevant director)



There will always be some changes that will be unrealistic. If you are responsible for them, try to keep away from these.
For example, we knew users will go on YouTube or Facebook during breaks.
Rather than use the Security policy document to explicitly forbid it, we permitted access under various conditions including, not during work periods, and only if it won't affect the business or other employees carrying out their work



And finally, don't go it alone.
If you're stuck, don't forget there is a community of specialists, some of who may have had the same battles you have.
You've got

- The Mac Admins Slack instance
- Conferences (like this one!)
- Local Meetups (such as our own London Apple Admins)

Looking to the future...

So, what about the future? What would we be looking to implement next?

Looking to the future...

So, what about the future? What would we be looking to implement next?

Looking to the future...

- Firmware passwords
- Unifying authentication systems
- Better data collection
- More documentation!
- More aggressive patching
- Spend more time with departments

moof IT

Firmware passwords
- These should be relatively easy to deploy
- Adds another layer of end device protection

Unifying authentication systems
- Perhaps using something like SAML or SSO?
- Or a cloud LDAP provider, perhaps JumpCloud?
- Would allow a central location to grant (or remove) user access, perhaps in the event of someone getting fired

Better data collection
- Collecting more logs and events-based alerts
- Cloud service and / or client based
- Options include Zentral
- Also considering intrusion detection solutions?

Documentation
- Fully document a user on-boarding and off-boarding process
- Plan and document user-level and company-level security incident procedures
    - e.g. what to do if you suspect your account has been compromised?

More Aggressive on the patching side of things
- Perhaps forcing user's onto the latest macOS around the new year period?
- TBC - Meltdown patched for latest OS only
- Suspect that Apple only patch 'everything' on the latest OS, despite releasing security patches for older OSes

Thanks

Q & A

http://www.moof-it.co.uk/technical/macaduk-2018-sup

Thanks to everyone!

Links:

- Mac Admins Slack - http://macadmins.org
- MacAdmin Podcast GDPR talk - https://podcast.macadmins.org/2017/12/26/episode-64-you-will-comply-with-ben-toms-and-reza-alavi/
- National Institute of Standards and Technology (USA)'s guidelines on handling digital identities, including updated guidelines on passwords - https://pages.nist.gov/800-63-3/sp800-63-3.html
- Unaffiliated site to check if a service might have 2FA - https://twofactorauth.org
- FileVault profile blog - http://www.amsys.co.uk/2017/08/profile-enable-filevault-2/
- Erik Gomez's Macbrained session (profile section) - https://youtu.be/nKgOWvC6p64?t=13m12s
- London Apple Admins - http://www.londonappleadmins.org.uk