

Welcome to our

August techshop



@myrtec

presentation overview

case study

what is MDM

benefits

implementation

best practices

summary



case study:

Bean Counters R Us

Bean Counters R Us is a Newcastle-owned and operated Accountancy Firm.

They have 25 staff, aged from 22 to 60 years old.

They have an IT provider but haven't updated their technology strategy in years. This is because Senior Management believes their IT systems are 'working' and they can't see the value in investing time or money into changing processes.

The younger staff at Bean Counter R Us disagree and rebel against company policy by using their personal devices for work-related use.

Some management staff at the company know this is happening but don't understand the risk. Others don't even realise employees are going against policy.



meet tammy.

Tammy is 28 years old Account Executive at Bean Counters R Us. Tammy uses her personal phone to store details for her work clients. This includes data such as their business names, contact details and, even their financials.

Tammy recently left her phone in an Uber and it was stolen. This made Tammy panic because she knows she has confidential data on her phone which was not backed up so she has no way to contact her clients. She knows her phone also stores confidential data that should only be accessed by people within her organisation.

A man with short dark hair and a beard, wearing a black suit jacket, white shirt, and dark tie, is sitting at a wooden desk. He is looking down at a stack of papers in front of him, holding a black pen over them. To his left is a silver laptop. The background is a wall of crumpled, light brown paper. The overall scene suggests a professional or business setting.

meet ethan.

Ethan is a 35-year-old Accountant at Bean Counters R Us. He has worked at Bean Counters R Us since graduating from University over 10 years ago and in that time has built a large portfolio of clients with whom he has great relationships with. He is ready to go out on his own and start his own Accountancy firm. He would like to take his portfolio of clients with him.

Ethan is going to copy out the information from Bean Counters R Us CRM and download it to his iPhone right before he leaves the company. From here, he will have all of his client's data saved to his phone and will email them all asking them to continue working with him, but through his own business.

meet lori.

Lori is a 56-year-old Senior Partner at Bean Counters R Us. She has been with the company for over 30 years and is very passionate about the work that they do.

One Friday evening, Lori was having a glass of wine at home when she received an email from someone claiming to be within her organisation. It was flagged with high importance and Lori didn't think twice before opening the link to investigate further details.

When Lori clicked on the link, it prompted her to log in to her Microsoft account. She entered her username and password but the site took her nowhere, so she put her phone away and gave up. It wasn't until Monday that she realised hackers had gotten into her Microsoft account and were threatening to release details if Bean Counters R Us did not pay a \$200,000 ransom fee.



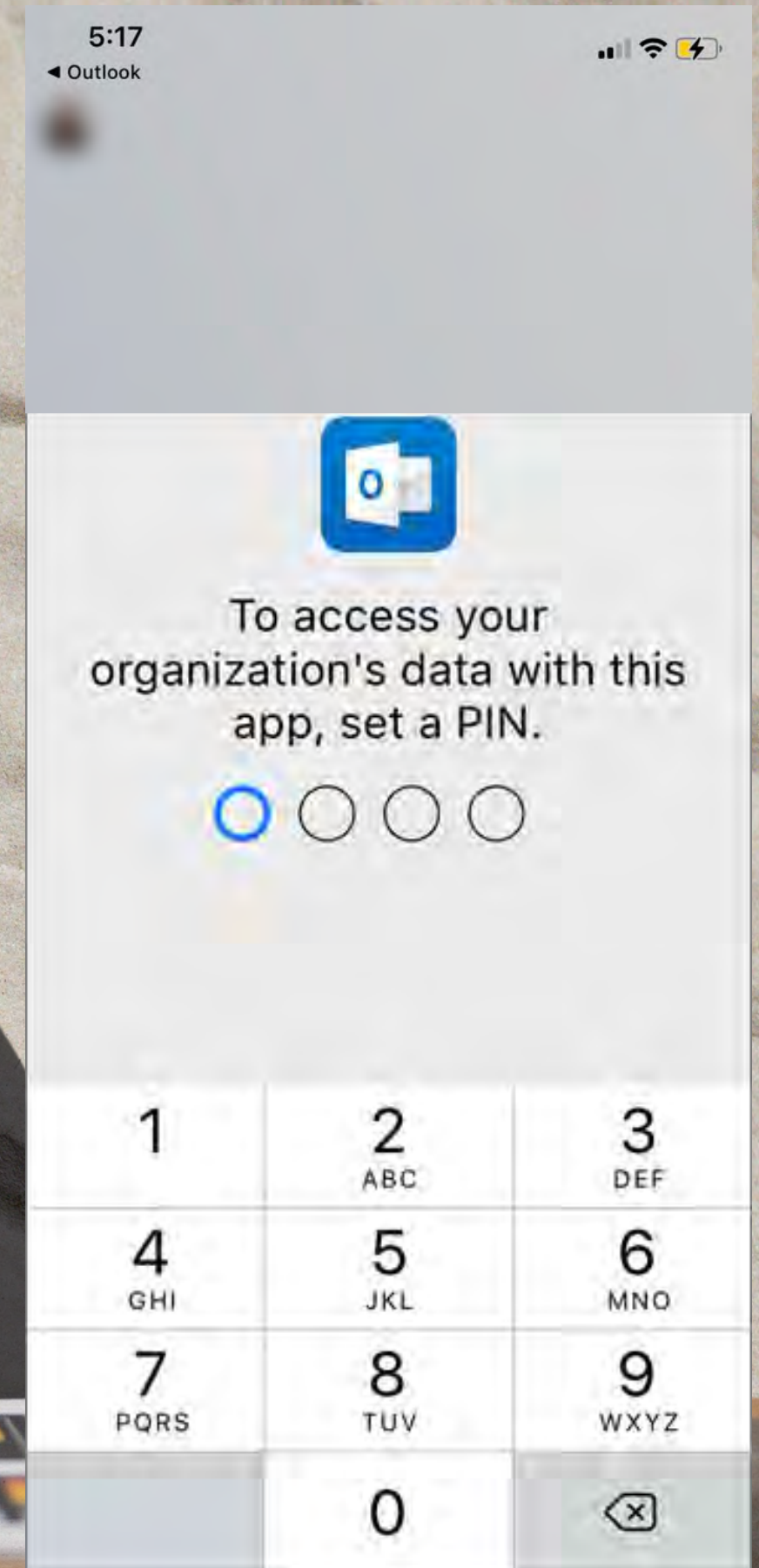
A diverse group of business professionals in a corporate setting. The image shows a large number of people, both men and women, dressed in business attire like suits and blouses. They are arranged in a group, with some in the foreground and others in the background. The overall tone is professional and positive, with many individuals smiling.

**what could have been
done differently?**

meet tammy.

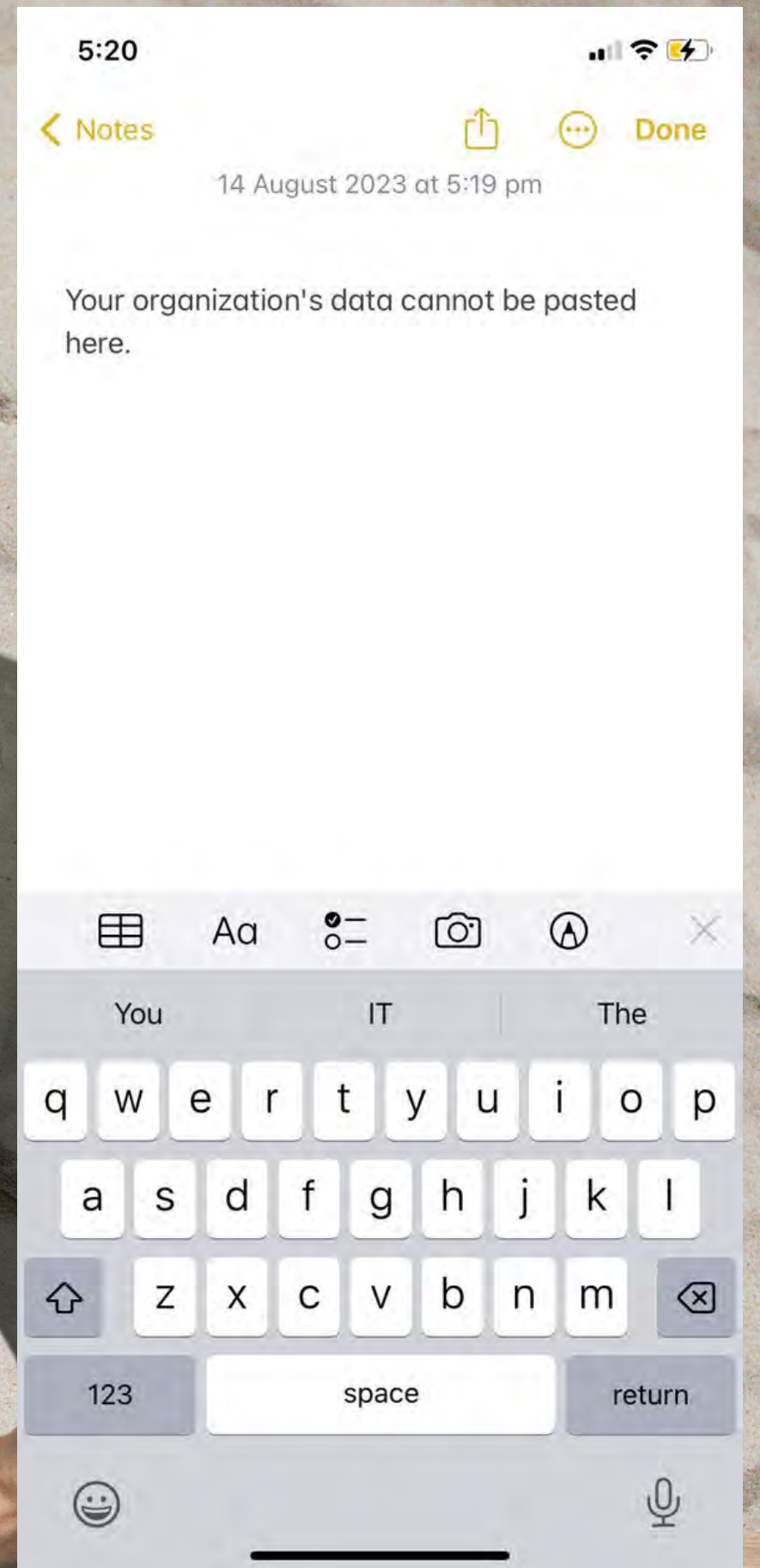
If Bean Counters R Us had an MDM policy in place, regardless of whether Tammy has a passcode on her phone, thieves still wouldn't be able to log in to her office accounts, such as Teams or Outlook, without a pin code or Face ID.

Her organisation could wipe the account from her phone remotely, confidently knowing no one was able to access the data on her phone.



meet ethan.

With an MDM policy, Ethan wouldn't be able to copy / paste or download any information from his work accounts onto his personal phone. It literally comes up with a message saying 'your organisation does not allow information to be pasted here.'

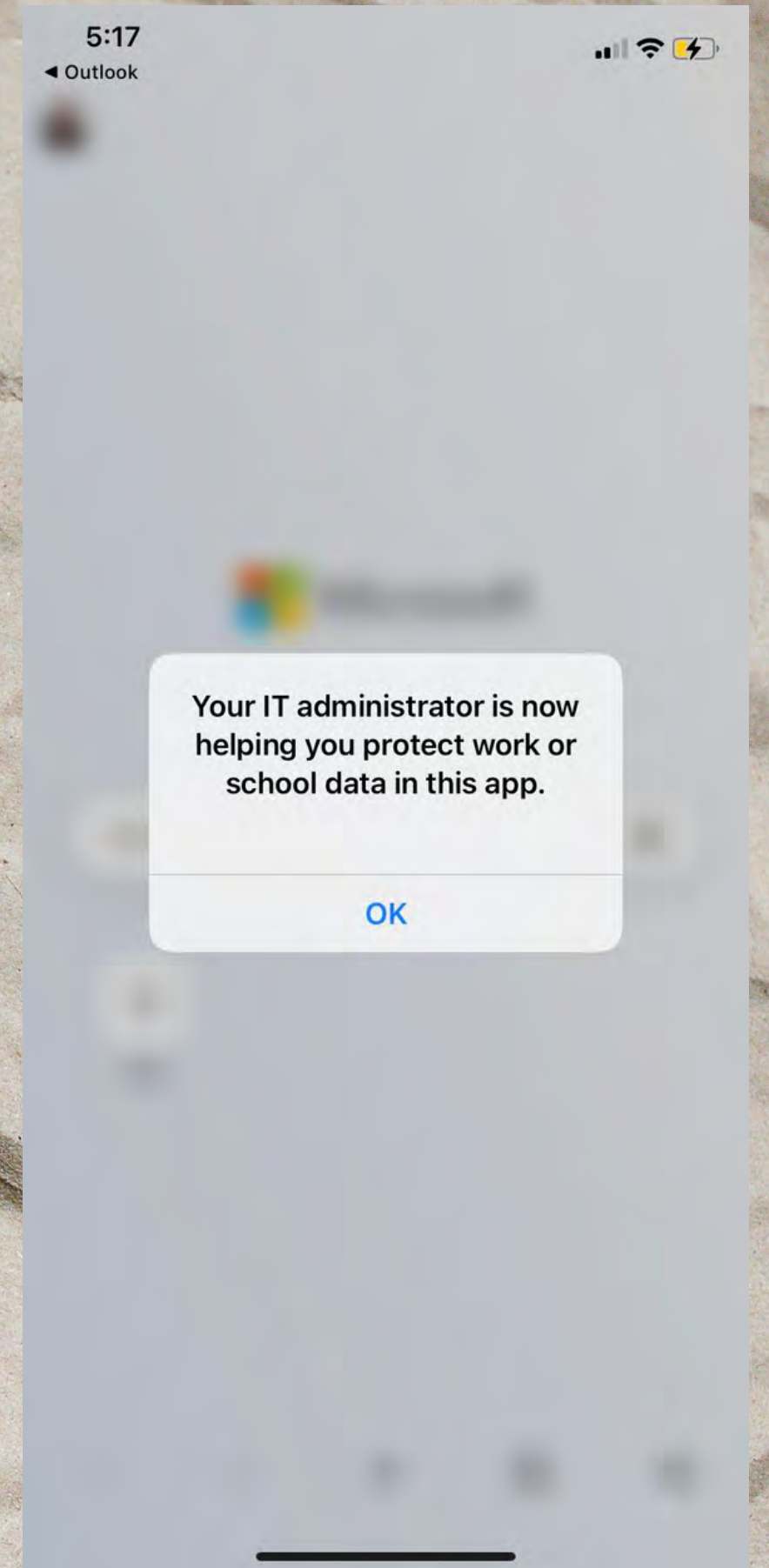


meet lori.


Lori is a 56-year-old Senior Partner at Bean Counters R Us. She has been with the company for over 30 years and is very passionate about the work that they do.

One Friday evening, Lori was having a glass of wine at home when she received an email from someone claiming to be within her organisation. It was flagged with high importance and Lori didn't think twice before opening the link to investigate further details.

When Lori clicked on the link, it prompted her to log in to her Microsoft account. She entered her username and password but the site took her nowhere, so she put her phone away and gave up. It wasn't until Monday that she realised hackers had gotten into her Microsoft account and were threatening to release details if Bean Counters R Us did not pay a \$200,000 ransom fee.



what is MDM?



a system to manage mobile devices (phones + tablets) remotely

ensures security and compliance

centralised control over device settings, app and data



why use MDM?



protects data from
unauthorised access

enforces strong passwords
and encryption

enables remote data wipe
in case of device loss



benefits of MDM

protects company data
against breaches

mitigates risk from stolen or
lost devices

tracks device activity for
auditing purposes

reduces IT support time with
remote troubleshooting and
automatic updates



setting up MDM



select an MDM solution. we recommend Microsoft Intune or Google.

enrol devices. this can be done remotely.

configure policies. passwords, encryption, app management + app controls.



implementation timeframe



can take 1-4 weeks
depending on company
size, complexity and
chosen MDM solution



costs to consider



licensing fees for MDM software

initial setup + configuration costs

ongoing maintenance + support expenses



MDM best practices



start with pilot on small scale
before full deployment

identify and address
challenges early on

educate employees about
MDM policies + benefits

encourage compliance for
successful implementation



summary + key takeaways

MDM is for enhanced security, improved efficiency and compliance

if you want a tech-forward workplace, you need to streamline device management

Speak with your IT provider about what MDM solution meets your company's needs

plan for implementation, address challenges and offer training



why you should work with myrtec



consolidated systems
are easier to secure

fast response to security
incidents

simplified information
management



September techshop

Register here



**Best Practices To
Ensure Your
Organisation is
Secure and
Compliant**

DATE | Wednesday,
September 20th,
2023

TIME | 12pm - 2pm

PLACE | Peibri Place
Function Centre,
97 Hannell Street
Wickham 2293

COST | Free but
registration is
essential

Thank you for attending our

August techshop



@myrtec