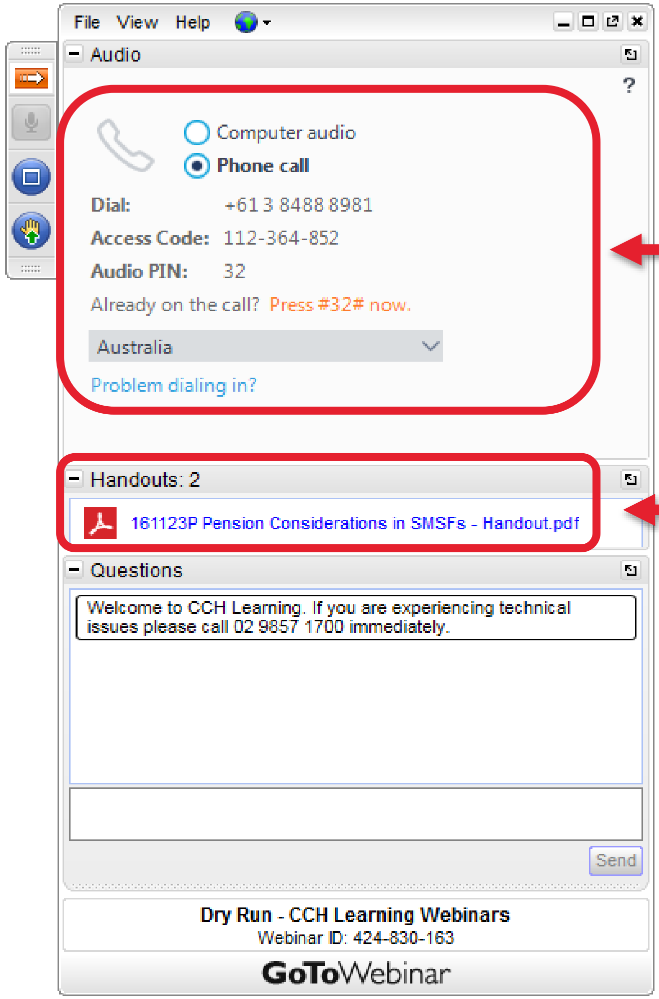
Bring Your Own Devices – Risks and Challenges

Tyler Wise

Tuesday 5 March 2024

How to Participate Today



Audio

○ Computer audio
● Phone call

Dial: +61 3 8488 8981
Access Code: 112-364-852
Audio PIN: 32
Already on the call? Press #32# now.

Australia

Problem dialing in?

Handouts: 2

161123P Pension Considerations in SMSFs - Handout.pdf

Questions

Welcome to CCH Learning. If you are experiencing technical issues please call 02 9857 1700 immediately.

Dry Run - CCH Learning Webinars
Webinar ID: 424-830-163

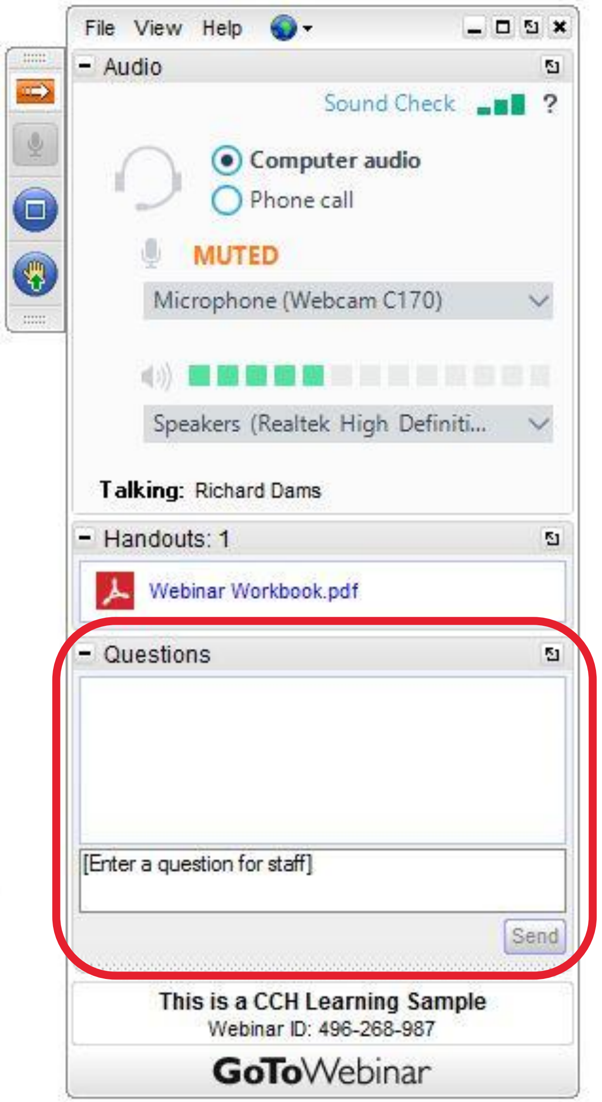
GoToWebinar

- Sound Problems? Toggle between Audio and Phone
- PowerPoint? In the Handouts Section
- E-learning Recording? Within 24-48 hours you will receive an email notification

Questions?

Susannah Gynther
Moderator

Type your question and hit Send



Audio

Sound Check ?

● Computer audio
○ Phone call

MUTED

Microphone (Webcam C170)

Speakers (Realtek High Definiti...

Talking: Richard Dams

Handouts: 1

Webinar Workbook.pdf

Questions

[Enter a question for staff]

This is a CCH Learning Sample
Webinar ID: 496-268-987

GoToWebinar

GROW YOUR SKILLS, GROW YOUR KNOWLEDGE, GROW YOUR BUSINESS.

Subscribe to CCH Learning and gain **unlimited access** to all live webinars, E-Learnings and supporting documentation.

Plus, your CPD hours will be recorded automatically.

Find Out More!

Your Presenter

- **Tyler Wise**
- Director
- Cyberwise

PRESENTED BY: TYLER WISE

CYBERWISE

BRING YOUR OWN

DEVICES

What is BYOD?

And why do we do it?

Governance based initiative to allow access to company assets and resources from decentralised devices.

It can afford significant cost savings to an organisation by reducing the amount of hardware required to be acquired.

Has been argued to result in higher employee productivity, job satisfaction, morale and convenience.

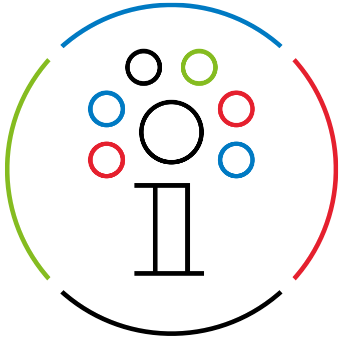
Less devices to be carried, and therefore lower risk of loss, and / or loss of company data.

Do you or your organisation allow Bring Your Own Device?

a) Yes

b) No

c) Special Circumstance



BYOD Risks

WHAT ARE WE 'BYODING'?

MOBILE PHONES

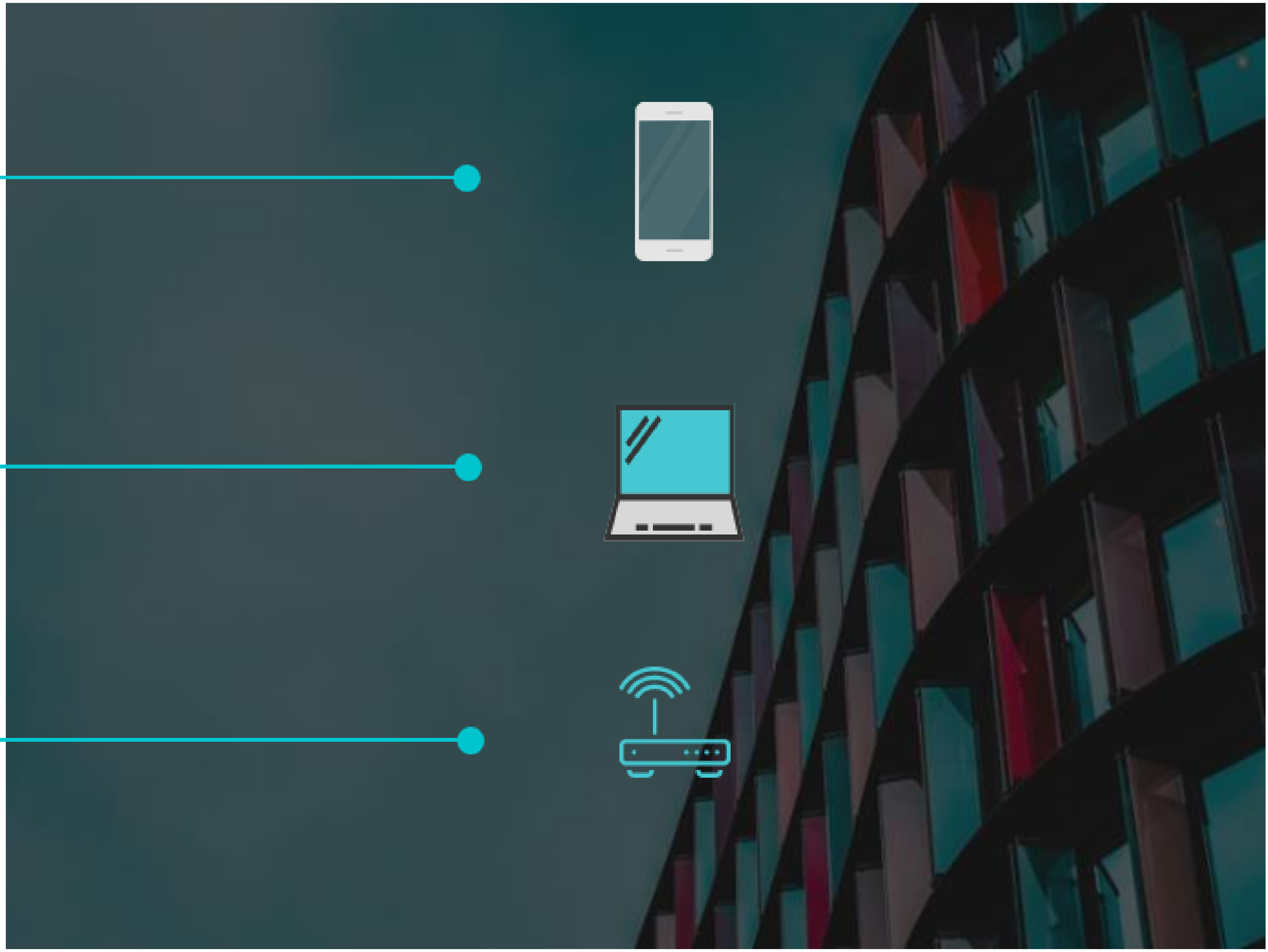
Ubiquitous and still expensive.

LAPTOPS

With team members sometimes having multiple devices, using an 'existing' one is easier.

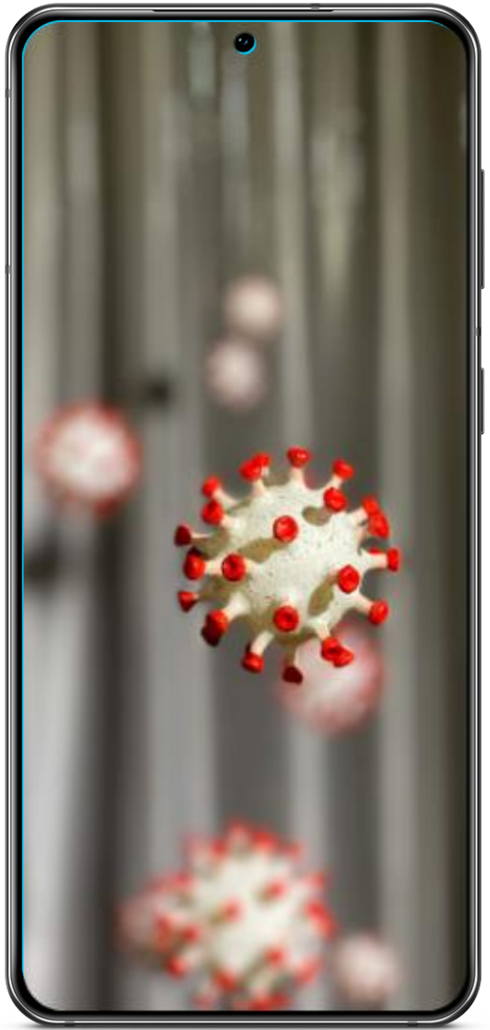
NETWORKS

Just connect and go...what is the worst that could happen?



Bring Your Own Device

A lucrative market, with more and more tools facilitating the growth.



$3,000,000,000

BYOD Market Value

$11,000,000,000

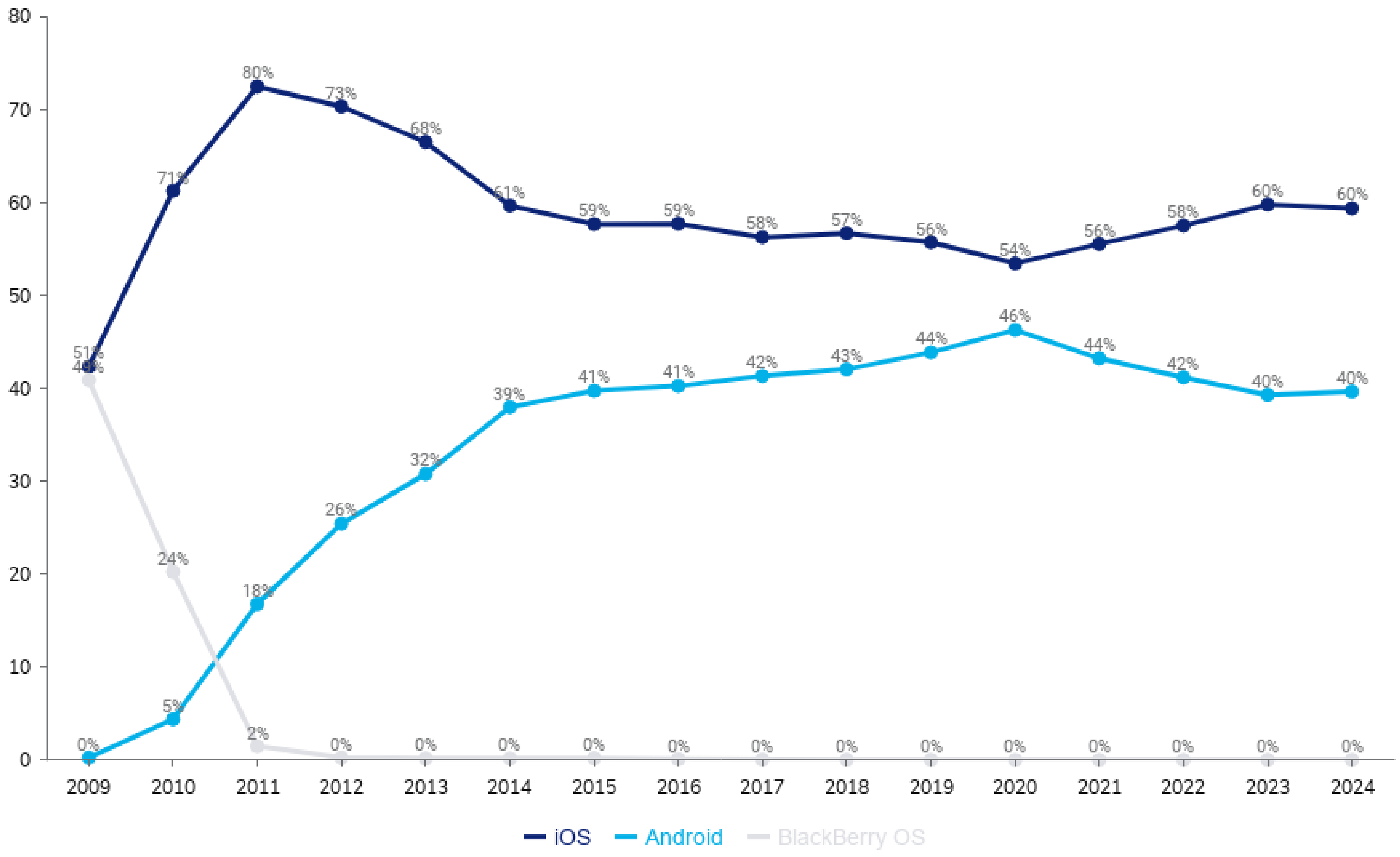
Estimated BYOD Market Value

Employees use of mobile devices for work purposes.

Employees use of mobile devices for work purposes.

MOBILE OPERATING SYSTEM MARKET SHARE AUSTRALIA

2009 - 2024



IOS IS BOSS

iOS holds the market share in Australia, which is contrary to the global trend. This affords some security benefits, but Android, still accounts for a significant percentage.

However, Apple
is not fully immune and some items to consider as warning signs:

1. Excessive or unordinary battery drain
2. Erratic performance or crashes
3. Unusual data usage

If unsure, check the status of your iPhone, update, and if all else fails consider a factory reset. The secure bootloader should ensure that no rootkits' exist on such a device.

Malicious Android apps with 1M+ installs found on Google Pl

By Bill Toulas November 1, 2022 04:0

lackers are sneaking malware on to
Google Play Store — how to stay safe

News By Anthony Spadafora published April 11, 2023

ven legitimate Android apps could be infected with ma

Comments (0)

36 Malicious Android Apps Found on Google Play, Did You Install Them?

They have been installed on Android devices nearly 10 million times and some are still availabl

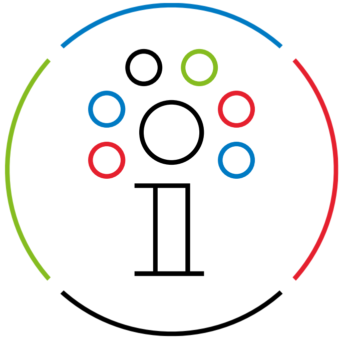
By Matthew Humphries July 27, 2022

Have you or someone you know ever sideloaded an app?

a) Yes

b) No

c) Sideloaded, what?



CYBERWISE

No need to root or jailbreak anymore...

- A tiny percentage of phones are either rooted or jailbroken, as most risks occur by circumventing device and organisation security protocols...

WHAT YOU CAN DO

IF A BYOD STRATEGY IS IMPLEMENTED HERE ARE SOME CONSIDERATIONS

01

SECURITY REQUIREMENTS

Ensure the operating system, and security measures are in place - and regularly checked.

02

APPLICATION DENIAL

If particular 'high risk' apps are present on an employee device, reject a BYOD policy for that employee.

03

GOVERNANCE STANDARDS

Ensure you have (updated) internal policies and procedures to ensure employee and device compliance with organisation requirements.

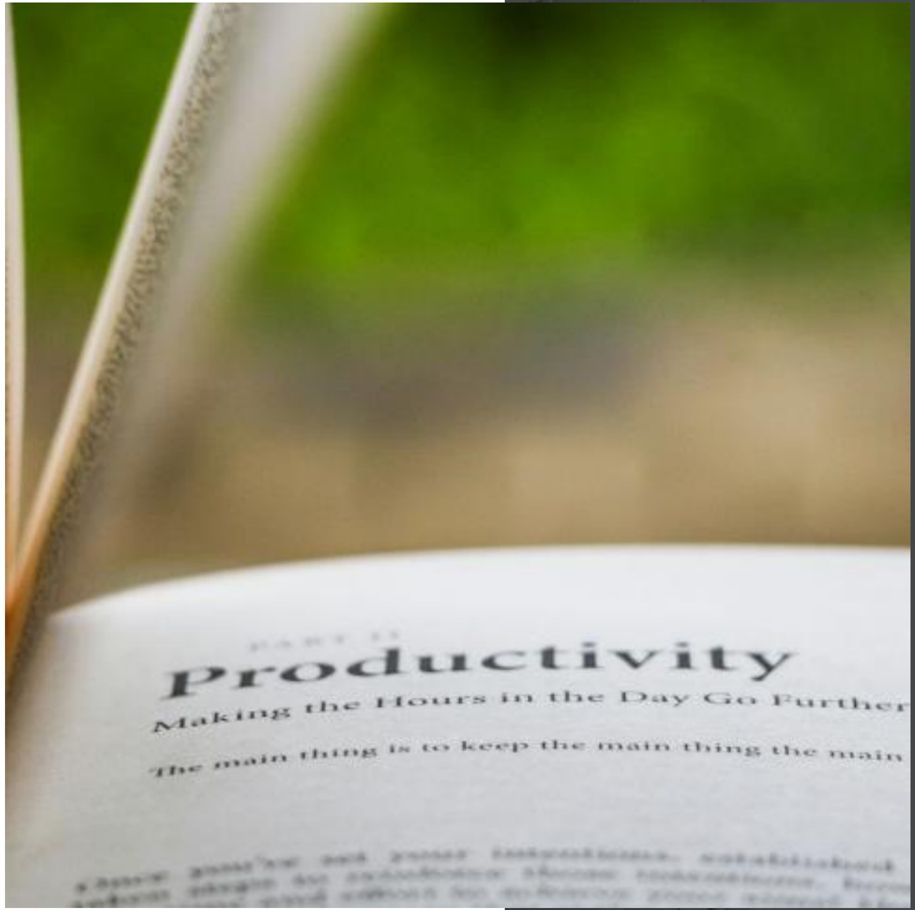
04

REGULAR AUDITS

It is critical that devices be regularly checked to ensure compliance with organisation standards and policies.

IS IT CRITICAL

Above all else, consider if connection to work resources from private devices is **absolutely necessary** for the employee to be productive.


Productivity
Making the Hours in the Day Go Further
The main thing is to keep the main thing the main

OUR CORPORATE PHONE USE

WHAT WE ARE LARGELY USING OUR PHONE FOR AT WORK...

Instant Messaging

This may be unavoidable, but consider what is shared across these platforms.

Passwords

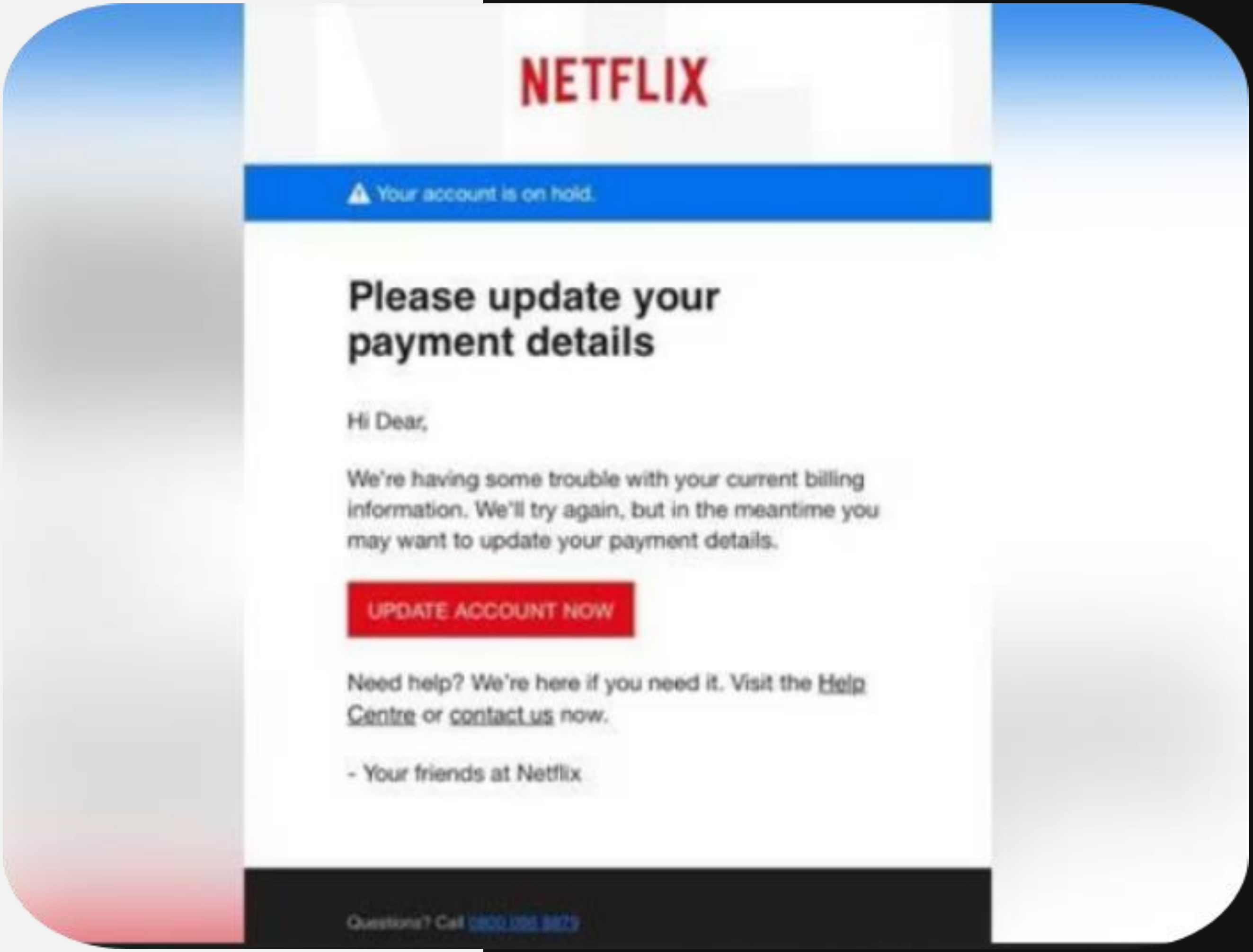
Are corporate passwords stored on a private mobile device a matter of necessity or convenience. Consider disallowing.

Authentications

Perhaps consider a different option, such as a hardware key, or desktop solutions - and definitely separate to your password manager.

Email

Is email access often a personal choice made, rather than a management directive. Many reasons to consider disallowing.



NETFLIX

Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call [illegible]

Lets consider an email example...

How could an email like this be more successful when accessed and actioned on our phone instead of our workstation?

____

___

- So, do we *really* need access to our emails all of the time?

WORKSTATIONS / LAPTOPS

Issues and what we can't control when it is not ours.

Who

The restriction of users is not able to be controlled when it is not a centralised device.

Where

If it's not yours, you don't where it is being plugged in and taken, which pose security risks.

Networks

No network limiting, and as such any networks could be joined by this device, at any location.

Site access

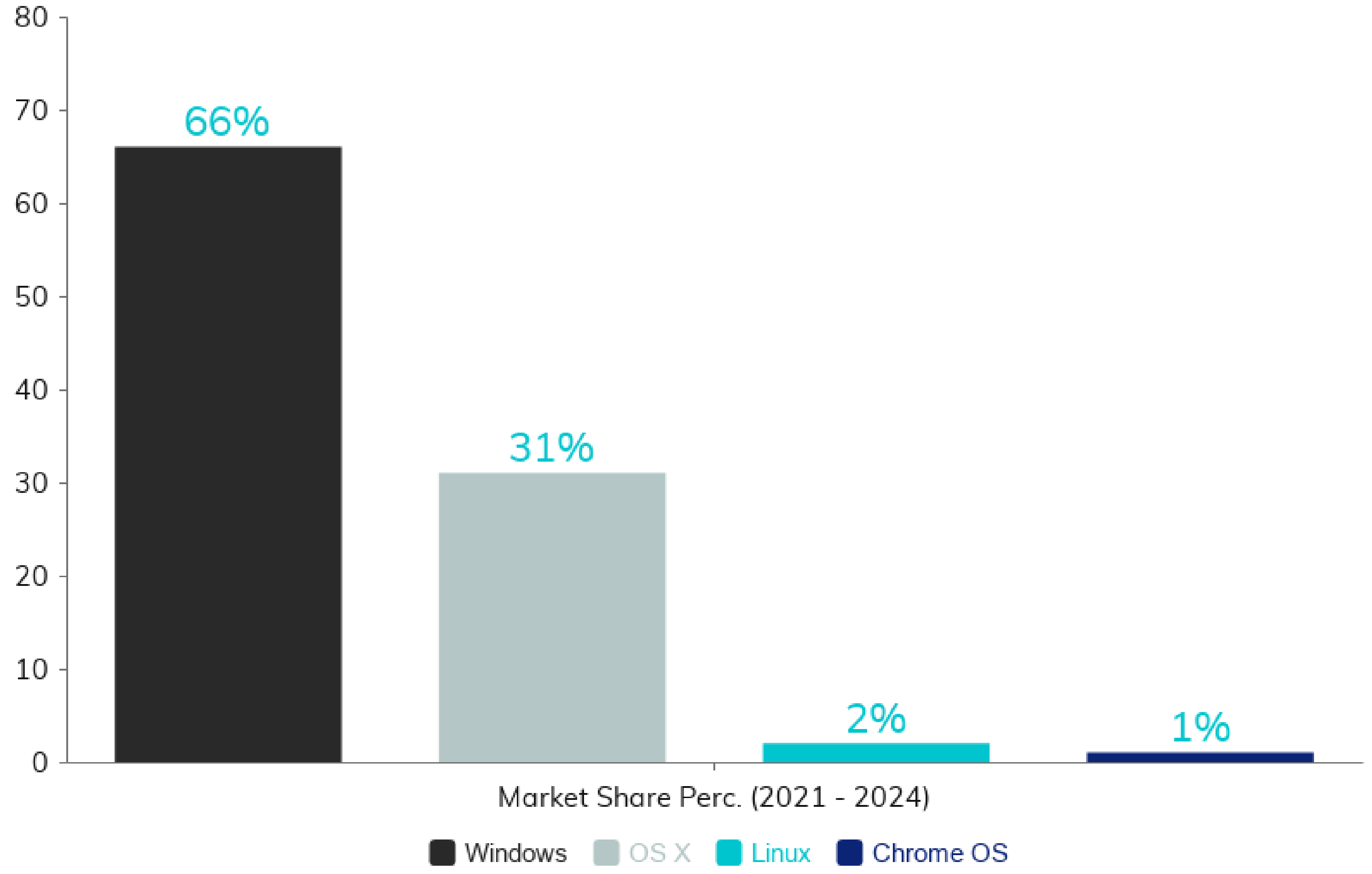
Any website could potentially be accessed from a decrentralised device, without strong governance.

Software

Cannot control the downloading, installation and executing of software on a decentralised device.

Desktop and workstation OS

KEY OPERATING SYSTEMS ONLY



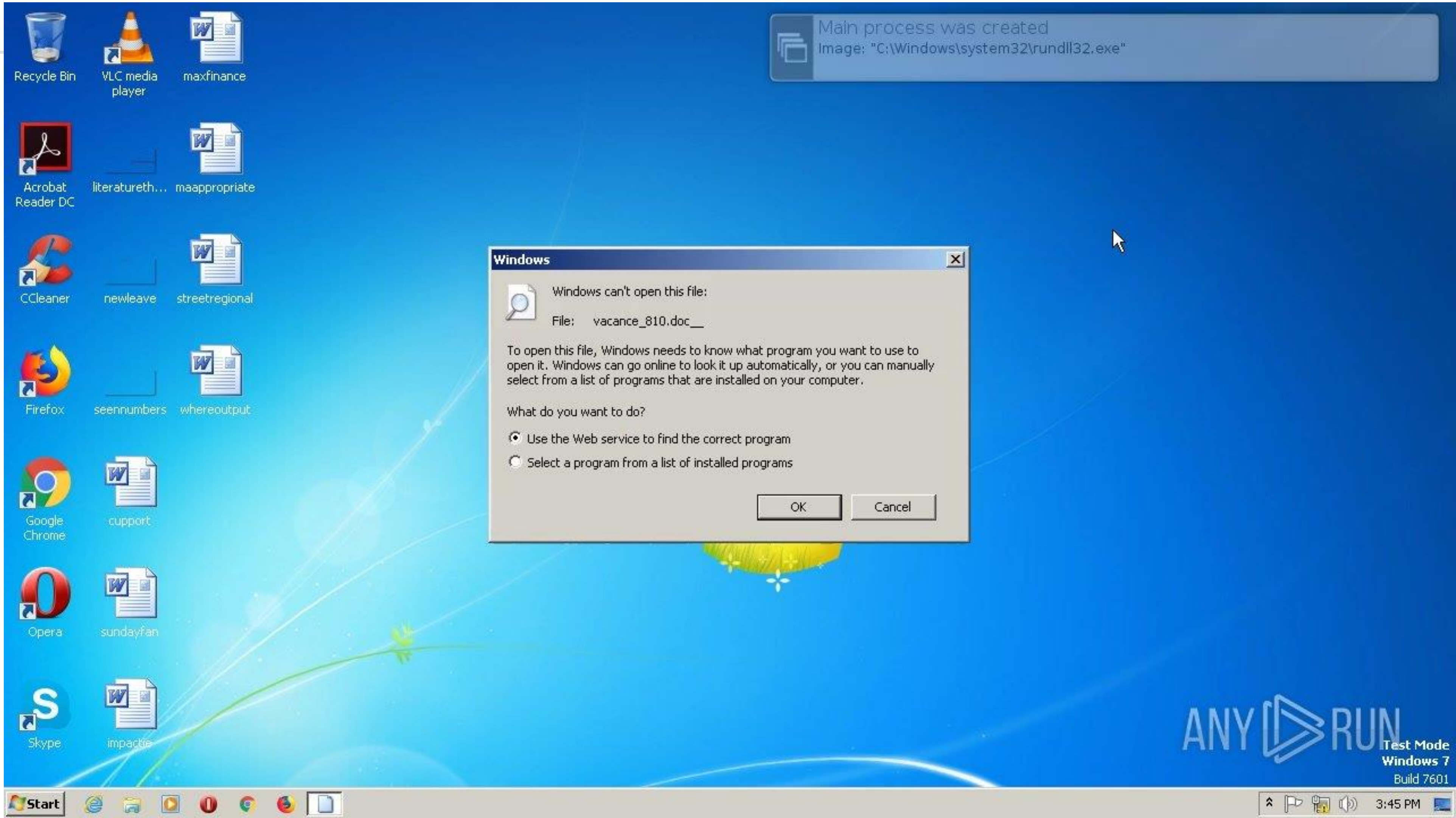
WINDOWS ALL THE WAY

No surprises that Windows dominates the enterprise space, and this is why there is significant risk. However, MacOS and Linux are not immune to risks. However they can be different and less widely exploited.

Deployment of the ASD Essential Eight are strongly recommended for any BYOD.

Let's see an example

RANSOMWARE AT WORK



Main process was created
Image: "C:\Windows\system32\rundll32.exe"

Windows

Windows can't open this file:

File: vacance_810.doc__

To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

What do you want to do?

● Use the Web service to find the correct program

○ Select a program from a list of installed programs

WHAT WENT WRONG

HOW WAS THIS ATTACK SUCCESSFUL...AND HOW COULD OTHER ATTACKS BE SUCCESSFUL?

PWNED

The machine is compromised, which could contain sensitive business data.

ADMIN PRIVILEGES

The file was able to execute malware as a result of the user having admin privileges.

NO VIRUS SCAN

There was no virus scan undertaken on the downloaded file.

POOR GOVERNANCE

Inadequate governance saw a malicious files downloaded from a potentially untrusted source.

CYBERWISE

HOW COULD IT LOOK DIFFERENT

BETTER GOVERNANCE AND / OR DEVICE CONTROL.

POLICIES AND PROCEDURES

Higher levels of control and rules providing governance about accessing unknown files on mixed use devices.

DATA AND DOWNLOAD CONTROL

Files and downloads can be controlled, and automatically virus scanned before being allowed to open; or third party downloads entirely restricted.

USER PRIVILEGES ONLY

Restricting user control means that the ability to install software and edit system files is denied or monitored.

ALERTS AND UPDATES

Suspicious or 'out of band' activity can be alerted to the organisation in real time to provide additional security measures.

NETWORK ACCESS

SOMETHING WE CONSIDER, BUT DON'T POLICE

What happens when we can't see it...

Our devices are constantly broadcasting and looking for networks to connect to.

Open networks offer no security to their users; and you never know who could be on the same 'line'.

Even secured private networks, such as employee home networks are not necessarily safe, as their are an average of 17 devices in a home now...and not all secured adequately.

It is possible to snoop traffic with minimal outlay and these can represent further risks.

BYOD CHALLENGE SUMMARY

THERE ARE MANY THINGS WE NEED TO CONSIDER WHEN DEPLOYING BYOD

1

COST

We cannot simply acquire new devices for every employee, budget constraints exist.

2

USER RISK

Employees may be less 'careful' (physically) with work devices than one they purchased themselves.

3

ENVIRONMENTAL CONSIDERATIONS

E-Waste is a major consideration when deciding whether to go BYOD or not.

4

TRANSIENT EMPLOYEES

Employees move between employers at a high rate, comparatively, and device management can be a challenge.

CYBERWISE

NAVIGATING THE LANDSCAPE

WHETHER YOU NOW SIT ON THE YES, OR NO, OF BYOD THERE ARE SOLUTIONS

— (NO) BYOD

Device control

Deploying company devices provides centralised control over applications and access.

Device Re-Use

Computing power is increasing, increasing the life use. It is possible to completely erase a device and re-deploy.

Governance needed too

Even when deploying organisation devices, there must be strong internal controls and audits to ensure compliance and security.

(YES) BYOD +

Must have governance

Strong internal controls are critical to ensure data and asset safety. Do not introduce BYOD without.

Data isolation

The access and storing of company data must be monitored and restricted to allow BYOD to be effective.

Checks and balances

A regular check of user devices is a must, ensuring operating system and minimum software requirements.

THE END

THANK YOU!

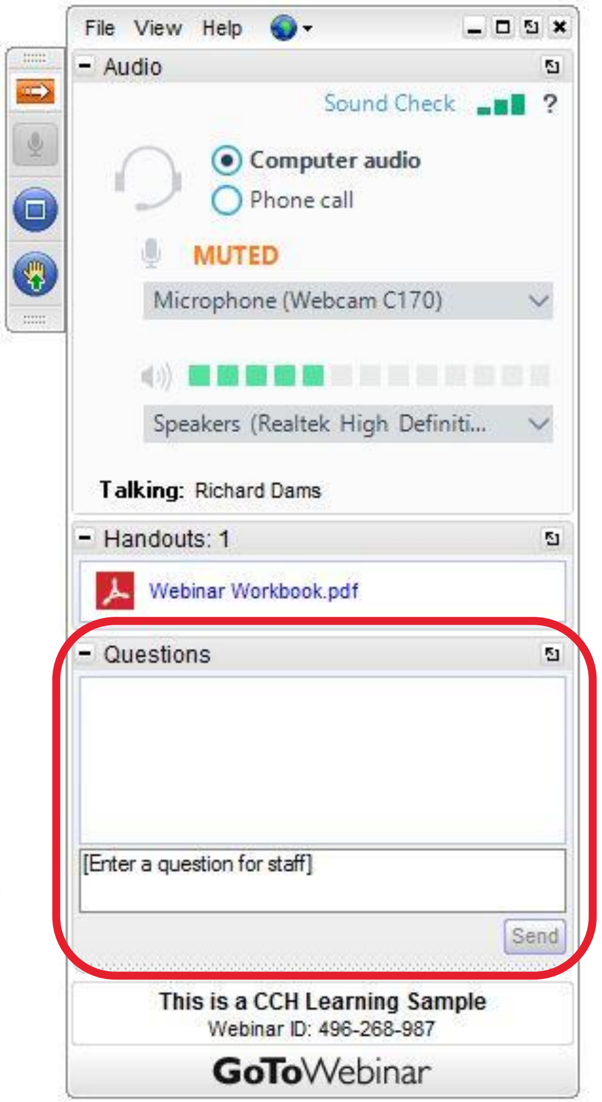
DO YOU HAVE ANY QUESTIONS?

We appreciate you taking the time to join us today, and hope you got benefit from the session.

Questions?

Susannah Gynther
Moderator

Type your question and hit Send



● Computer audio
○ Phone call

MUTED

Microphone (Webcam C170)

Speakers (Realtek High Definiti...

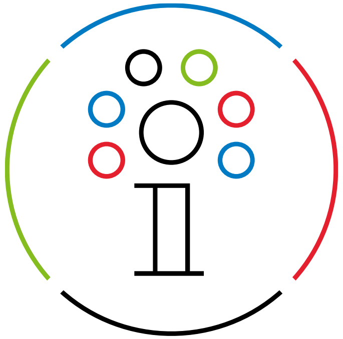
Talking: Richard Dams

Webinar Workbook.pdf

[Enter a question for staff]

This is a CCH Learning Sample
Webinar ID: 496-268-987

Upcoming Webinars



View all Webinars

- 5 March – How Best to Extract Funds when Selling a Business
- 6 March – Couples, Care and Considerations – Understanding Aged Care
- 7 March – Income Tax Case Update
- 7 March – Non-commercial Loss Rules for Individuals
- 13 March – The Ins and Outs of Super – A broad look at Contributions and Pensions
- 13 March – FBT 2024 – Understanding Entertainment and Meals

Questions

- Tyler Wise
- Director
- Cyberwise
- 02 5016 9999
- tw@cyberwi.se

Next Steps

Please complete the Feedback Survey.

Within 24-48 hours you will receive an email when the following is ready;

- E-Learning Recording
- Verbatim Transcript
- CPD Certificate
- PowerPoint Presentation

Thank you for attending

Wolters Kluwer

CYBERWISE