CWSI

Harnessing the power of Mobile for your Business

In Early December CWSI hosted a panel discussion on harnessing the power of mobile for your business. CWSI are a Dublin headquartered mobility consultancy, offering many services, professional services and training to many respected organisations across a wide range of industry and public sectors in Ireland and the UK.

Ronan Murphy
CEO
CWSI

Philip Harrison
CTO
CWSI

Paul Line
Commercial Director
CWSI

Contributing to the webinar were:

RONAN MURPHY - CEO, CWSI

With over 25 years' experience in the Mobile Telecoms arena, Ronan has been involved in multiple start-ups and subsequent business disposals over his career. As an established thought leader and market strategist in mobility, he has been invited to participate as judge, panellist and speaker at various mobile technology events. Ronan has provided strategic advice to many of Ireland's leading corporations in the area of Enterprise Mobility and has acted as advisor to numerous vendors wishing to participate in the Irish market.

PHILIP HARRISON - CTO, CWSI

Philip has over 15 years' experience in the IT service sector with a strong educational foundation in computer science – a Computer Science graduate of Trinity College, Dublin. His experience ranges from first-level user support to major infrastructure consultancy to management. Philip worked with customers of all sizes in all major vertical markets and is recognised as the leading authority in mobile IT in the Irish market.

PAUL LINE - COMMERCIAL DIRECTOR, CWSI

Paul has extensive commercial and operational experience in Information Technology & Telecommunications, retail and also FMCG sectors within both privately and publicly held businesses in the UK, Australia and New Zealand. During his time in Australia, Paul was instrumental in growing a disruptive, start-up IT & telecommunications business to $80M of revenue and a successful listing on the Australian Stock Exchange.

Topic Overview

In a recent survey of 650 IT decision makers from around the globe, three quarters of companies are currently undertaking digital transformation initiatives - 80 percent of those companies said if they don't finish their initiatives, they will lose revenue in the coming year.

It is clear the consequences of failure are high, as firms spend a great deal of time and money figuring out the most effective route to business and digital transformation. But sometimes they overlook the most powerful tool available, one that's right in the palm of their employees' hands — their smartphones. So, let's explore how firms are harnessing the power of mobile for their businesses and learn how you can do the same for yours.

PHILIP HARRISON, CTO

In 2019 things got smarter, smart business, smart tech, smart mobile.

Endpoints are endpoints are endpoints. Technology has progressed enough that a single management solution is now the smart choice to manage all your endpoints, from smartphones to desktops to MacBooks.

There are three areas we saw movement on in 2019. The first was around the management of endpoints.

The term "Unified Endpoint Management" (UEM) has been knocking around for a few years now - it's basically the idea that a single unified management platform should be able to manage your smartphones, tablets, Windows desktops and Mac desktops. In 2019 we really started to see clients take this seriously. It's no longer a matter of us trying to persuade businesses that UEM is the right way to go, they're actually coming to us demanding it and asking how it can be done.

Fortunately, I think the technology is now mature enough to make it happen. The likes of MobileIron and VMware have credible UEM offerings, and we're seeing Microsoft slowly suck SCCM up into InTune, to create a single cloud-based endpoint management platform. My message on this one is that UEM is now the smart choice for businesses of all sizes. What we've been doing for the last 10 years is focussing particularly on the management of mobile devices, the smartphones and tablets. Most businesses would already have some sort of solution for managing their desktops, and that solution has probably been in place for 20 years. Then they will potentially have a platform for managing Mac, if they've welcomed Macs back into the enterprise as well.

> **“Most businesses would already have some sort of solution for managing their desktops, and that solution has probably been in place for 20 years.**

Three separate platforms, all very different. There's definitely opportunity now to combine them into one platform. In terms of the end-user experience, it becomes seamless to transition between these different devices and platforms. But we need to think from the business side as well. It's less vendors to manage. It's easier to have your admins trained up to manage one platform, looking at a single pane of glass rather than three separate platforms. All across the business, it's more efficient, and a smarter way to go.

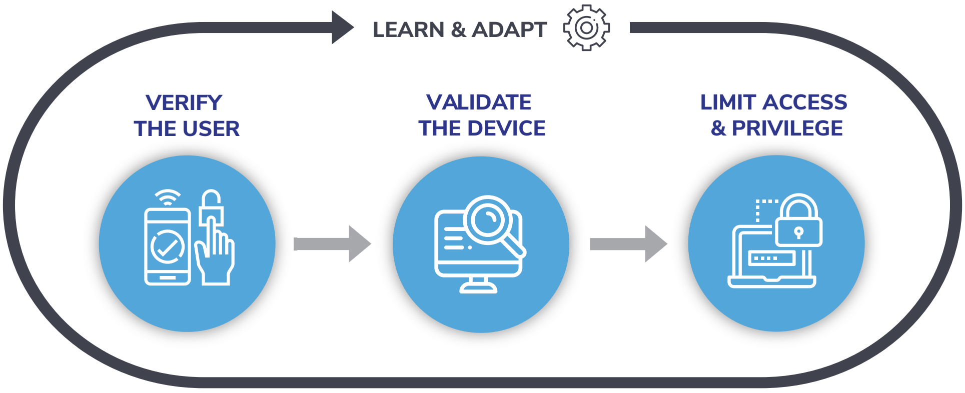
> “Zero Trust is the concept of not trusting users once they’re inside, but instead constantly verifying them at different stages.

Passwords and perimeters were never enough. Unequivocally trusting users inside your network with a valid password is now a broken security model; Zero Trust has become the catch-all term for the solutions, but some of them really are smart!

Zero Trust. It’s very much the latest piece of cyber security jargon I know, but there is some sense to it. It’s a reminder that the old model of building strong perimeters around your network and trusting anybody who makes it inside, is just no longer valid.

Firstly, your data has moved out to cloud services and mobile devices, so even defining your perimeter is virtually impossible. Then phishing attacks on users have become so advanced and so common, that you really can’t assume that a user with a valid password is who they say they are and should be allowed run-riot in your network. As an example, a security consultancy we work with recently mentioned to me that they are dealing with one case a week of phished passwords being used to access cloud systems – that’s pretty crazy for a small practice!

So Zero Trust is the concept of not trusting users once they’re inside, but instead constantly verifying them at different stages, preferably without requiring them to re-enter credentials, because as we’ve already said these cannot be trusted anyway.



If you look at the likes of the Microsoft DMS platform, there’s a feature called conditional access in there, which is like a rules engine that when you do your single sign-on, it’s looking to see if you’re coming from an unusual location, or maybe you’re logged in from London one minute and five minutes later, you’re logged in from Brussels - an unusual activity. Then it can prompt you for an extra factor authentication or can check if you’re coming from a device you don’t normally come from. Maybe it’s an internet café and the system decides you should just be allowed to read data not download it.

You can do a risk assessment when the user logs in to figure out what they should have access to. The idea of zero trust in an enterprise setting is that you’re hoping not having to re-authenticate too much.

> 91% of Fortune 100 companies now use Microsoft Teams.

91% of Fortune 100 companies now use Microsoft Teams. The march to cloud services seems unstoppable now that all reliability and credibility questions appear to have been answered. Cloud First is now firmly the smart business choice.

My last one then is just around the continued move to cloud services, and I'll say the least about it as I think we're all very familiar with how fast this is happening. Microsoft Teams has been a really interesting case though. Realistically what Teams does has been available for years in products like Slack, but the fact that Teams is so easy to turn on and roll-out to desktop and mobile if you already have Office365, it's being seen as a no-brainer by most businesses.

We've had a number of high security clients, who would never have considered cloud services in the past, dip their toe in the water because of demand for Teams. And once that floodgate is open you see more and more services move to the cloud.

If you're already using Office 365, and virtually every business out there is using something in Office 365, to turn on Teams is just a click of a radio button and off you go. To do that securely, there's a bit more involved in there to do it right but it's very easy, whereas you could try to persuade your users to use slack you can be difficult enough to even get used to put it on the phone most teams just seems natural to people. Cloud First and Mobile First are the new normal for smart businesses in my opinion.

Keeping pace with the pace and rate of change...

Most cloud and mobile-solution providers are heavily incentivised to get their customers onto the latest versions of their software; they want to have fewer software versions to maintain, and they want to reduce their risk of security breaches against people using old vulnerable code.

At a risk of sounding like my sales-y colleagues who are about to speak, I think the best way to deal with the rate of change here is to outsource as much of the mundane day-to-day stuff as you can, to allow your talent focus on the strategic stuff and staying up-to-date with advancements. And for this strategic stuff, have a partner available that knows the space and can boil down the jargon for you.

> The best way to deal with the rate of change here is to outsource as much of the mundane day-to-day stuff as you can.

For a number of clients, we do "centre of excellence", where we would meet with the customer and some of their stakeholders once a quarter and talk through some of the advancements in Office 365, Mobile or whatever solution they're using. You can field questions from the client and from different parts of their business. You're trying to get people from marketing and sales into those meetings and we share our insights into how they might utilise the technology better.

“What we’ve really seen through 2019 going into 2020, is that the war for talent continues. Our customers have started using technology to help attract that talent.

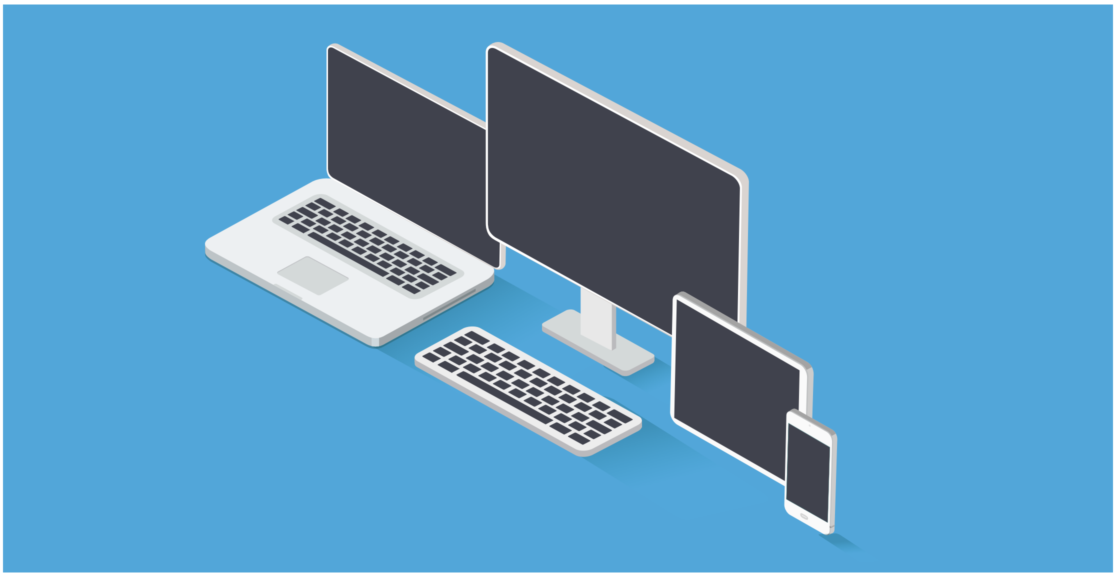
RONAN MURPHY, CEO

How business can take the “smart” advantage in 2020 and win the war for talent.

The war for talent – why putting employee experience at the centre of your IT strategy will help you win.

What we’ve really seen through 2019 going into 2020, is that the war for talent continues. Our customers have started using technology to help attract that talent, and they’ve begun to recognise that devices like Macbooks and iPads and iPhones are what new starters expect to have when they arrive in a business. These new starters don’t like to be driven towards specific types of technology.

You’ll see on social media a lot of these unboxing videos being shared - new interns joining a business and opening the smartphone and opening the computer and the tablet or iPad that’s presented to them. It sounds like a very small thing, but in these people’s lives, they like to use the technology they’re comfortable with they like to use the applications they’re comfortable with. Driving them down a specific technology avenue is not always the right thing and can really go counter to a good experience and good engagement with employees.



We’ve had situations with big professional services companies where they’ve said MacBooks have to be adopted into the organisation to facilitate these new graduates, and to get them to sign up. Having the technology that can manage MacBook and Microsoft and iOS and Android is really important for companies going forward.

> The goal is happy employees, working better and being more productive.

The goal is happy employees, working better and being more productive. Teams need to be able to use multiple devices, to collaborate and work with those devices with their colleagues, whether they're in the office or at home, and obviously, all of that has to be done with security and compliance in mind.

Mobile is everything now and security & compliance have taken centre stage.

I was watching Marc Benioff, the CEO of Salesforce at Dreamforce last week. He had Tim Cook from Apple on stage and he was telling the group, and telling all the attendees and those watching, that he doesn't own a computer anymore. He uses iPhone for everything. He said, "Look, I do have a computer, but I don't know where it is. It is somewhere because it's got some photos I want to keep on it. But," he said, "for my day to day life, I use my iPhone, I connect to cloud services, and use apps and I can do everything I need to do as the CEO of an organisation like Salesforce."

I think that just shows you where we've come to.

If we think about security compliance, and about Marc Benioff using a laptop that wasn't secured with all the security controls that are standard in enterprise IT, you'd be shocked. But there's probably people like him using iPhones for all sorts of things. And they haven't looked at that security and compliance piece around it.

It's really important that we remember that it's the responsibility of the security resources within companies to make sure that they have a comprehensive mobile security framework in place, that can automatically scan every device, every network and every cloud service.

> What we often see is projects being stalled because of lack of security sign-off.

When we look across our customer base is amazes me when we come across new customers who haven't thought that through in the world of mobile but have a secure story. I'm from traditional IT, but mobile is so visible today that it's now becoming the heart of everything. We've all seen victims of data and security breaches. How do you put client's minds at rest when it comes to security? Getting firms, that maybe won't make the decision to deploy mobile, over the hump.

What we often see is projects being stalled because of lack of security sign off. And it's really the fact that businesses are not educated or informed about the array of mobile threats there are. There was a feeling that Apple and iOS, because it was a walled garden, was a safe environment. I think there's been multiple incidents over the last few years to show that that isn't the case.

When we join a lot of these projects, which are stalled, for security reasons, we're able to say, look, here's how you can mitigate that security risk. We can bring you on a journey where we'll take out that security risk and give you a compliant user, that enables productivity, using security in the background to make sure it can happen.

Decisions around the Digital Workspace have moved beyond IT – HR, Legal, Marketing, Sales all have a voice that needs to be heard and need to be aware of security risks.

The decisions around the digital workspace have moved beyond IT. We've found, in our engagement with large organisations, a lot of the projects that stall are with IT and IT security. It's not really a pure technology conversation with IT anymore. It's really important that Legal, Marketing, Sales and HR are involved in these conversations.

HR understand what the people they're recruiting need and want.

Then Legal makes sure that the policies that the company want around IT usage are applied to mobile, and sometimes there may be very different policies for mobile usage, because you have a larger cohort of employees using their own device and stacks as business resources. How are legal covered off on that area?

> Marketing and Sales are keen on using iPads to collect data, as iPads get a better response than a traditional clipboard.

Marketing and Sales are keen on using iPads to collect data, as iPads get a better response than a traditional clipboard. We've seen, in in multiple healthcare environments, people are more comfortable talking to someone gathering their information on a digital resource than they would be on a clipboard.

Involving all those different parts of the business in in the digital workspace, as opposed to just traditional IT, is really important as we move forward. I remember a couple years ago we were working with a council in the UK. The IT director said that he only owned 55% of the technology budget. The balance belongs to the CEO, using digital technology to make the council more productive and serve the public better.

> I think those cultural challenges are nearly as important as the technology challenges.

The IT department is still really, really, really important as the security folks, but how can we use this new technology, that's in everybody's hand and everybody's pocket, to enable our organisations better, to give a better service to our clients and to give a better productivity suite to our employees, who are working for us every day.

It's not just technology that's changing fast...

There's a cultural challenge along with the technological challenge. With organisations we work with, we're fortunate enough to work with a lot of the Tier One Banks in the UK and also that the retail banks in Ireland. More often than not, the technology is there, and they know it's there, but it's a cultural change.

People only using a corporate owned device, and only using it for the limited access they have - That's a challenge for them when they know they can communicate much better by using shadow IT. It's a cultural challenge to get new people coming into the bank to understand that they don't have something like Microsoft Teams, or they don't have something like slack.

One of our banking clients moved to a new office facility and home-working blends. The idea was that some people would work three days a week in the office and two days from home. The technology is there to do that, but there's cultural challenges around someone who may have worked in the bank for 30 years, and they are used to going into their desk and sitting down. All of a sudden, their job is work from home. I think those cultural challenges are nearly as important as the technology challenges.

CWSI are very happy to help arrange how this is all communicated to employees.

PAUL LINE, COMMERCIAL DIRECTOR

Why going mobile never made more sense - make money / save money.

The cost of replacing employees is huge – the right tools are key to employee engagement and retention.

The war for talent really is an ongoing challenge, not only to attract the best people but to keep them. CWSI know, and research backs this up, that technology is a key reason why people choose to work for an organisation. It's also a key influencer in someone's decision to leave an organisation.

We also know that the nature of work is changing, work is an activity, not a place. When we talk about work technology, we're more often now talking about a mobile device, tablet or laptop than a powerful desk-based PC or a larger monitor!

According to research from Forrester:

80% of millenials say workplace technology influences their decision to join a company.

42% indicated they would change employers if not provided with technology that meets their needs.

> “When we talk about work technology, we're more often now talking about a mobile device, tablet or laptop than a powerful desk-based PC or a larger monitor!

It's worth taking a second to think about the cost of that to an organisation. Consensus seems to be at least £5,000 in direct costs to the business on average, but it can be many more times that depending on the level of the employee and how they're recruited.

In simple terms, consider an organisation with 1,000 employees. Reducing turnover by 10% would save at least £0.5M annually. Additionally, there are soft costs that impact on your “employer brand” that are harder to quantify but are still real.

For example, what's the cost of all those negative employee reviews on employment sites like Glassdoor? How much harder does this make it to attract talent in the first place? What impact does this have on the morale and engagement of the people who stay?

> **There are no longer jobs for life, or even for 2 years. Just look at the rise of the gig economy, the increased use of short-term contractors and global, agile teams.**

The right technology strategy can help to address all of the key drivers of the cost of on-boarding:

- On-boarding paperwork and admin - great new tools such as VMWare's intelligent assistant enable companies to streamline the contract acceptance and technology choice process
- Technology Provisioning during on-boarding - OOBE (Out of the Box Experience) - shipping devices directly to new users
- Early leavers - the right provisioning sets the tone early and gives confidence
- Deferred productivity.

The nature of employment also continues to change. There are no longer jobs for life, or even for 2 years. Just look at the rise of the gig economy, the increased use of short-term contractors and global, agile teams.

I firmly believe that getting good at this stuff will become a strategic capability that can differentiate a business.

The productivity advantages of a mobile-first approach are significant – these have a direct influence on your bottom line.

Productivity benefits work on a couple of different levels. Firstly, and by far the most importantly, it's worth thinking about at an employee level.

Ask yourself this simple question - what do I need to do to log-on to and access all of the information I need to do my job?

- How many systems do I need to access?
- How many usernames and passwords do I have?
- What security hoops do I need to jump through?
- What constraints are there that stop me accessing these?
- Where I am?
- What kind of connection I'm on?
- What device I'm using?

Philip touched on a couple of key things - Unified Endpoint Management and a Zero Trust approach to security. The premise of Unified Endpoint Management Solutions is to enable EASY and SECURE access to any data, application or information, from anywhere, at any time and on any device.

> Ignoring the Digital Transformation opportunity will end up as a business cost.

A very simple example of the benefits is something like single sign-on and self-managed password re-sets. They:

- Reduce the time taken for employees to access key data
- Reduce the time taken managing passwords and any associated downtime
- Reduce the knock-on impact on the service desk

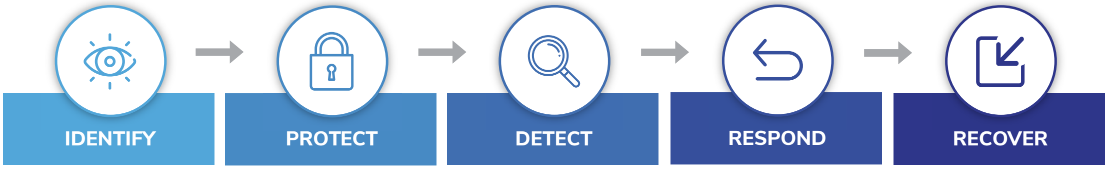
Consumer Simple, Enterprise Secure

The second level is an internal IT level. Unified Endpoint Management provides a single pane of glass for IT to be able to manage ALL endpoints. The cost to support multiple, disparate solutions is much higher than a unified or integrated solution. Often the internal costs of supporting such a solution are higher than using an external expert.
Ignoring the Digital Transformation opportunity will end up as a business cost.

Investing in strategy lowers your total costs – Measure twice, cut once to speed up your digital transformation, avoid wasted effort and realise productivity benefits more quickly.

One of the most common questions we get from our clients is "Where do I start?"

Don't start with the technology or with procurement. We see lots of CFOs starting with an objective of reducing licensing costs, but this is putting the cart before the horse. Our answer is to start with your business goals and objectives and work backwards. What are you trying to achieve and why? A good example might be "to be more responsive to our clients' needs". Perhaps they'd like to "give our customers peace of mind through better security" This could be aligned to achieving a security standard such as NIST or ISO27001.



NIST Cyber Security framework.

Build a plan. Summarise your goals and objectives are and where you currently stand.

Involve the whole business. This is not just an IT responsibility, the opportunities (& threats) are at a business level. The line of business leaders needs to be driving initiatives from the top-down.

Then assess the capabilities of your existing technology & alternatives.
Many organisations have technology that can support their business goals but just aren't maximising value from it.

> Can you put a price on trust? The value in being a trusted organisation should be prioritised over ROI.

Firms will want to end up with a technology Blueprint or roadmap that aligns with their business strategy.

User personas can be incredibly useful:

- What types of users are there within your business?
- What do these users need?

An ROI that delivers more than "Bottom Line"...

ROI is often focused on efficiency and on cost-savings, and while these are important, it's also important to look at how you can drive the top-line. How can your technology enable more sales, better customer service, customer retention, customer responsiveness?

For example, giving a sales manager the ability to quickly approve a sales discount for a new deal, from anywhere via a mobile device with one-click, can drive more sales and better customer service. Perhaps giving a front-line worker the ability to flag an additional job that needs doing, to a salesperson, and producing a quote in minutes, can drive better customer retention.

Can you put a price on trust? The value in being a trusted organisation should be prioritised over ROI.

Concluding Remarks

PHILIP: Firms need to consider the security challenges around Office 365. All these cloud solutions and mobile solutions are difficult, but solvable, and I think the key is to engage someone like CWSI to help you navigate those waters.

PAUL: This is far too important to leave to just IT. Make sure that you involve the broader team of key business stakeholders in whatever you're doing to develop your strategy in this area.

RONAN: Businesses should treat mobile seriously. It's an opportunity to grow your business, make your employees happy, it's not a headache, and it's not something that should be treated as a headache.

How can we help? Let's explore how we can leverage our expertise and experience to help you achieve your commercial objectives and stay secure in a mobile first world.

cwsisecurity.com | info@cwsi.co.uk | @CWSI_IE