Bring Your Own Devices – Risks and Challenges
05/03/2024

CCH Learning:

Hello, everybody and welcome to today's webinar, Bring Your Own Devices - Risks and Challenges. My name is Susannah Gynther from Wolters Kluwer CCH Learning and I will be your moderator for today. Just a few quick pointers before we get started. If you're having sound problems and can actually hear me, please toggle between audio and phone. Hopefully if you are having sound problems, you can see that instruction on the screen. If you are looking for the PowerPoint for today's presentation, it's saved in the handout section on the GoToWebinar panel.

Just a reminder that shortly after the end of this session, you will receive an email letting you know that the e-learning recording is ready to be viewed. You can ask questions at any point during the presentation by sending them through the questions box. I will collate those questions and ask them at the Q&A towards the end of today's presentation.

CCH Learning also offers a subscription service, which many people have termed, "Netflix for professionals." It provides members with access to our entire library of recordings as well as live webinars for a competitive flat fee. That's for over 500 hours of content. For CPD purposes, your viewing is logged automatically.

Your presenter today is Tyler Wise, director of Cyberwise. Tyler is a seasoned professional with over two decades of experience in the fields of public practise accounting, cyber security, and open source intelligence. With a diverse background that includes being a former owner of an accounting practise and the founder of the cyber security firm called Cyberwise, Tyler possesses a unique perspective on how cyber security integrates into a business model.

Throughout his career, Tyler has honed his expertise in various areas including forensic accounting, digital forensic, and OSINT, open source intelligence investigations. His deep understanding of these fields enables him to provide valuable insights and solutions to businesses seeking to navigate the complex landscape of cyber security threats. I will now hand you over to Tyler to commence today's presentation.

Tyler Wise:

Thanks, Susannah, and welcome everybody. I'll just make sure I share the right screen, which seems to be working.

CCH Learning:

Yep.

Tyler Wise:

Does that work? Yep. Great. Awesome. I'm just going to check that. Sorry, Susannah. Doesn't look like video is showing up, so I'll talk over that one when we get to that one.

CCH Learning:

No worries, thank you.

Tyler Wise:

So thank you for joining us today, everybody. And what we are going to go through is something that's very relevant to a lot of organisations globally, and also locally in Australia of course is the bringing your own device. So it's really enabled the scaling of many, many businesses and something that I guess has really grown a lot of legs since Covid. So we get some efficiency gains when we do this for obvious reasons, but with that comes some cyber security risks. And what we want to go through today is just having an understanding of those risks and then some initiatives we can put in place to help us make sure that we navigate this safely really.

So when we think about Bring Your Own Device, it's really a governance initiative that allows employees access to company assets and data through the use of their own devices. So I think most of us are fairly familiar with the term, and again, about 83% of organisations offer some form of bring your own device initiative or strategy. So again, I think the ground worker that is fairly well understood by most people. Now the reason for its popularity is it works on both sides, employee and employer. From the employee perspective, it affords some significant cost savings because the hardware life cycle is elongated because we're no longer using our own devices, we're sort of piggybacking off those employee devices and giving them access to the data and the assets that way. So all of a sudden the requirements to acquire this hardware are drastically reduced and again, we saved some money that way.

It has been apparently proven to be resulting in higher employee productivity, job satisfaction, morale and convenience. And that might just be wrapping up that cost saving in something that benefits the employee because again, how you quantify that is questionable but again, that's what a lot of the research and studies suggest that is the case. But one genuine risk as well as a hardware perspective is there's less devices to be carried and that lowers the risk of losses of the device and or the company data information. So I think we've all been through a period where we had carried multiple phones and it's easy to forget one or you leave one at home and you just wish you had access to the other one or whatever it might be. And so we also know that generally humans are a little more protective of their own assets, things they bought with their own money compared to company equipment. So we do have those added benefits of that.

So that is kind of what bringer end device is in a nutshell. I think most of us, again are very familiar with it. What we really talk about though is the risks that we are exposed to when we deploy a Bring Your Own Device governance initiative. So I want to start off just with a really quick poll just to get a lay of the land and that is to see if you or your organisation allows a Bring Your Own Device policy. So I guess Susannah, just pop up the poll please. Three simple answers. So yes, no, or only in special circumstances.

CCH Learning:

Certainly. So I'll just launch that poll. So yes, just put a click next to the radio button that best describes your situation. That would be really great. And just a reminder that if you do have any questions, please put them into the questions pane and we will get to those at the end of the presentation. Okay, I'll just give you a few more moments to get your votes in there and then we'll close the vote.

Okay, I'm going to close it and let's have a little look there. 50% said no, 30% said yes with 20% saying special circumstances. Back to you, Tyler.

Tyler Wise:

Awesome, thank you for that. That's really interesting. Such a high percentage sit in the no side of things. At the same time, while that might be bucking the global trend, I think it affords you some additional cybersecurity measures that you just don't get when you've got your own devices or employee's own devices out in the wild. So we'll talk about those in a bit more detail. And really what we know is that there's three areas we're bringing our own devices to. The first is mobile phones. So we know that because obviously having multiple devices is really expensive, a lot of parity exists. So the functionality, you don't necessarily need special devices like we perhaps did back in the day of BlackBerry's and the like in order to get corporate email on the run. But what we sometimes think when we are thinking about, oh, we'll just use the employee devices is because we're not necessarily thinking about it from a functionality point of view, but more a convenience point of view.

And so, by that I mean we're thinking that we need to provide our employees with the latest iPhone as an example, or the latest Android or Samsung device when we need to bring it back to the functionality, what do we need them to do on this device and therefore what is the minimum device that we can give them? Again, making sure that adheres to these security protocols that we've got in place so they can do their work. So by that you can save some cost savings at that point by not having to go to the latest and greatest. It is always nice to have shiny new toys, but when we're dishing out company assets, maybe we can lower those cost expectations by simply not having the high-end hardware. Again, that's if you're going to go down that path. If your employees bring their own devices, that's entirely up to them what they have, we are going to talk about what we need to expect from that.

Now, laptops and workstations. These make a lot of sense because we just don't want this graveyard of computers and I know some organisations have a very simple policy that when somebody leaves that computer is effectively trashed and a new one is provided to the replacement employee. So we see that hardware costs, those cycle costs go up a lot. We probably don't need to do that, but more or less we avoid that. So we let employees bring their own devices in, they log into the network, they access company data, they work on company data all on their own laptop and we move forward that way. Again, we really can repurpose that laptops. I don't think we need to worry about the fact that hardware has gone at such a rate that an old laptop is no longer suitable. The computing power is definitely accelerated, but what we need to think about is do we need all that power?

So similar to the phones, thinking about the capability of the device, a lot of work that is done especially with software as a solution, so a lot of browser-based work, we don't need high-powered computers. So something with not exceptional RAM and storage is still going to be sufficient for us to get the job done. And as long as the computer doesn't look beat up or anything along those lines, there's no reason it can't be safely sanitised, being that wiped, and then provided to the replacement employee down the line. So again, we can navigate those costs there by thinking about how we're going to use the hardware and really extending its life.

But at the same time there is now an expectation amongst employees that they just can use their own hardware. Again, the whole work from anywhere work style has facilitated that and that's what we tend to see occurring now. And then finally, the one we don't always think about when we're thinking about bringing your own devices, but that is networks. So we expect employees to more or less provide their own network, which is fine in some instances, but we don't really ever police this and it's something that we need to consider. And again, we're going to talk about it a bit, but this is an element of bring your own device that we just need to be monitoring really, really closely because we just can't control what occurs on that network, who's on that network. And as a result of that, there's some fairly significant risks that we need to be thinking about.

And a lot of the solutions that we can put in place are really centred around really sound governance. So you don't have to be a technical expert in order to facilitate a really robust bring your own device strategy. We've just got to make sure we've got the words on the page that keep everybody accountable and we've got those checks and balances in place. Now, there's no small sums as bring your own device market. So in 2019, before it sort of took off, it was worth about $3 billion and 60% of employees were using their own devices for work purposes. But-

CCH Learning:

Tyler, I hate to interrupt you, but can you just share your slides? They seem to have disappeared.

Tyler Wise:

Sure can.

CCH Learning:

If that's okay.

Tyler Wise:

There we go. Thank you.

CCH Learning:

Thank you, Tyler.

Tyler Wise:

Excellent, thank you. So we can see. So now I'll just bring up mine. Yeah. So we fast-forward to 2026 and it's going to effectively quadruple up to about $11 billion. So there's a significant amount of acquisitions and that also factors in as well the work that we'll do behind the scenes as the employers. So this is not just simply everyone buying a lot more phones and computers, this is things we need to do in regards to network segmentation, ensuring security protocols, virtual private networks, all of these sorts of things. So the bring our own device landscape is going to expand and really, really impact our businesses as we go forward. So we don't really expect it to disappear. And we can see by then about three and four employees will be using their mobile devices for work purposes, which we probably expect most people do that, but again, not everybody does.

And it's getting to the point now where these laptops and smartphones and internet of things are so ubiquitous that it is inevitable that we will start accessing work data from our own devices if we're not already. So what we've really got to do is make sure we're being really deliberate with that. And we're going to go through now and talk about some phones that we want to talk about and analyse. In Australia, because we are a bit of a higher wealth country, we sort of buck the trend. So you can see here on the screen that Apple iPhones effectively account for 60% of the mobile operating system market and Android is about 40%. Now globally, you flip that around and it's 60% to Android and about 40% to Apple. So the reason for that again is because of the decentralisation of a hardware for Android devices.

So we know you can go to the post office and buy a really cheap Android phone for about $100. You cannot go and buy a cheap phone that will run iOS. It just doesn't work that way. So we are all familiar with the Apple wall garden and as a result of that, it does afford us some additional security when we're thinking about bringing our own devices because it is so heavily policed and regulated. I know some people find that very, very frustrating, but at the same time it does afford us some security. So those additional hardware costs do come back in spades and provide some free security, I guess if you like, for lack of a better term. Now, Android again offers some higher customization and by its own nature the operating system itself is open source. So we've got these many more players in the market and of course many more applications as well because it's just not so heavily regulated.

Fairness to Google, they are trying their hardest to effectively make Google as safe and sound as Apple, but there's still a long way to go.

Now, often when we think about these people, oh great, we're an Apple organisation so we're completely safe. It's important to understand that these Apple devices are not completely immune, but you'll get some fairly obvious indicators of compromise if your iPhone has been compromised. So the first one is always the accessible unordinary battery drain. So we tend to notice that and we'll often think, oh, the phone's on its way out, we need to get another one. But again, really monitor it and think if has it only happened since I installed a particular application or did I open a file? Again, it's not immune to malware. So we've got to still be having our shields up and thinking about this.

Erratic performance of crashes. Now that's one again, we tend to think, oh, the phone's on it way out. But again, before you start thinking like that, I just implore you to ask the question, have I installed something that I perhaps shouldn't have? Should I have click somewhere, or shouldn't have? Is there something happening in the background that's causing these crashes or the device to constantly reboot or shut down? And then of course the number one that we always notice is when internet charges are going up, so it's constantly sending out data. So when those phones don't really have that firewall, but you can put security measures in place for that. But that's how you can check your iPhone and they're very manual easy checks to put in place because you're getting those, I guess those almost tangible indicators. With Android, you can effectively follow the exact same concept.

If you're going through your battery a lot quicker, apps are crashing or there's unusual data usage, it could indicate there's malware on your device. Now as far as Google goes, it's easier to get malware onto Android devices. Again, there's a huge amount of applications globally. Again, it holds the lion's share. So there's a lot of people working to build malicious apps. It's unfortunate, but it's true. And we can see here on the screen here that the Google's own Play Store is responsible for a significant amount of malware infecting devices. So it's something to be constantly. And even just the other day there was five applications that were removed from the Google Play Store that were effectively file viewers. And we see this with Android and also with Windows devices where people are installing an application as malware under the assumption or the hope that it's effectively a productivity application.

So a big one is PDF file viewers. So on your phone you might not be able to view a PDF file, so they download something, but really that's just going to go through and read all of the documents and files within your phone or there's a phone cleaner, so you want to tidy it up and get it working a bit better. And so that says ask for permissions to your files, to your contacts, your messages, all of that so it can tidy it up, but really what it's doing is grabbing that information and sending it back to a control centre. So something that we've just got to be really, really mindful of. And we've got, I guess another risk when it comes to Android and that is the ability to sideload applications. So what that means is you more or less can download an APK file, put it onto your phone, normally you'll download it from your phone, click on it and instal it that way.

And that is not being checked by Google, not necessarily checked by the device, your installer and who knows what that's doing? So that's something you just cannot do with Apple devices, but it is something that you can do with Android devices.

And I think we'll start with a second poll. Our last poll as well is to find out if you or someone has ever sideloaded an app. So by that, have you downloaded an application, that APK file, put it onto your phone and used an app that way. So more or less tried to avoid using the Google Play Store or you may have a jailbroken iPhone installed an app that way. So I'll get Susannah to pop up that poll please and just a yes, no or I've got no idea what sideloading is.

CCH Learning:

No worries. So I'll just launch that poll. So as Tyler was saying, please click in the radio button and let us know what your answer is. And just a reminder, if you do have any questions to please put them into the questions pane and we will get to those questions in the Q&A at the end of the session.

I'll just give you a few more seconds to get your votes in and then I will close the vote. Okay, I'm going to close the vote now and let's have a little look, shall we? So 60% said sideload. What? With 20% saying yes and 20% saying no. Back to you Tyler.

Tyler Wise:

Awesome, thank you. And I'll just make sure I share my screen this time. So that's actually reassuring for me that so many people have got no idea what sideloading is because it really reduces those cybersecurity risks that we are talking about. Now, it has gotten a lot easier these days. Now don't worry about this video, we're going to watch this in a second. But more or less what you used to have to do in order to do that was to either route your device, so by that, get admin privileges or jailbreak it if it was an iPhone. So we don't see that really as a threat anymore. It's about 0.014% of devices that are either rooted or jailbroken. So again, it is really encouraging from a security point of view. I think that is also reflective of the landscape in that people using these devices for sensitive information and doing this effectively circumventing these inbuilt security functions is not something that's very advisable and they know this and so we're not doing it.

So what we need to think about then is again, these Android devices and how easy it's to circumvent the security features with them. So I want to show you this video now that I have done now. I'm going to talk over the top of it, so I might pause. I did have it prerecorded, but we had some issues getting it working this morning. Now effectively we've got three devices here on the screen. So Apple on the left, a dumb phone in the middle, and then an Android phone on the right. So we'll get rid of the Apple iPhone and the dumb phone because they don't really hold the... The dumb phone doesn't hold the information that we want, which leads us to the Android device, which does pose a risk. Now within this, you might not know what sideloading is, but what you need to be mindful of is the fact that perhaps one of your employees will, or who users are bring your own device or maybe they've got an old phone and they want to tidy it up before they start using it to access company information.

A lot of these times when malware ends up on a phone, it is by accident. So I don't want to sit here in my ivory tower and accuse everybody of doing something malicious. I think a lot of the times it is very much accidental. Now within the Google Play Store, you can see it on the screen, there is Play Protect. So effectively what that will do is scan the phone and scan the applications and see if there's any malware present. So in this instance we can see no harmful apps found on their test device and the recently scanned apps are all listed there. Now this is a really positive feature, a really great feature. The risk is, that you can see here, that you can easily turn this off. So if this is my device, I can choose to turn this off because maybe I want an application that Google's sending me a warning, but a friend recommended. I know it's fine, I just really went on it. I'm going to switch this off.

What happens is a lot of people when they switch these off, they don't switch it back on and then your phone is basically exposed constantly. So these are features that we need to ensure are permanently on and especially if we're giving employees access to our information because without that, again malware is very, very easily installed. So I'll just wait for me to finish talking on the screen there. So we can move forward as well, and when we go searching for an application as well, we're given additional data. So Apple really introduce this, and I'm picking on Grammarly here, but you can see when you get to the app and you scroll down, it tells you what it's going to do, be that good or bad. So we can see here data is encrypted in transit, which is a good thing. Other times it will tell you it's tracking a whole bunch of information.

So I have picked on Grammarly because we might think it associated as a productivity application, but within some cyber security circles it's a disallowed application because it is effectively a keylogger. So albeit the data is encrypted in transit, but we don't know who's accessing that data. And you think about what you type into your phone, you're probably typing in passwords. So again, Grammarly might be something, an application you want to disallow. What you can do here is we can download an APK file, and this is how we sideload those apps. So effectively there's lots of places where you can download these. As you can see here, I've simply searched for Grammarly within the APKMonk website and then it's just got this download APK. So it's just a matter of downloading that file, that APK, it will go straight to my downloads' folder. So again, Android and Apple, they have these, it's not too dissimilar to a computer these days. From a file system structure, we can see here it's going to download it and then all we have to do is navigate to the file directory and we're able to instal that.

Now again, there are APK files for a lot of things and you might think why would I do this? But people do it because you can get paid applications for free by downloading the APK. And obviously, it's no different to when you power up software, you've got to be really careful because if it's free, you don't know if it's being altered. There's often no hashes to check, not that people do that on mobile phone devices. And so you run these real risks. So this is why people will download APK files because Grammarly, again, I'm picking on it, you can just go and get that from the Google Play Store, it's free. But other applications that are paid, you might not want to pay for it until you'll go to a site like this to download it. So we can see here, we can see in the downloads file that it's there. I appreciate it's a little bit blurry from the visualizer, but what we get here... I'll just see if I can get rid of my bar.

I have received a prompt now. So the latest Android devices will come with some additional security features. So this is effectively the Samsung device saying we're not really going to allow you to instal this because it's come from an untrusted source. So this is a security measure that new Android devices have that say you cannot sideload applications. So we might get excited by that and think that's fantastic. The risk is of course, here we are given the option to cancel or hit settings, and effectively we just go to settings and then we can allow it to do this. So we turn the permissions on and that would effectively download or instal that APK file and we've got no idea what's going on in the background. Once that is installed, normally the application would be there, so in this incident it would be Grammarly, but we don't know if it's a legitimate version of Grammarly and what it could be doing.

So the reason I show you this is because when this is... If I'm working for you and I'm bringing my own device... I'll get rid of that video there. It's just sort of saying that we don't need to worry about Apple or dumb phones. If I have my own device and you give me the ability to access my emails or access company files from this, that's great. You don't know if I'm turning these security features on or off. Now again, you only need one person to circumvent your entire security policies. So as we always say in cyber security, you have to play defence all day. The attackers only have to score once. So we've got to be really, really careful with this and police this. So if an employee has an Android device, we need to audit it. We need to make sure those features are permanently on before we give them access to this information, because it simply carries too much risk.

And that is why there's a few simple steps. And if we're going to do this, some considerations that you need to put in place. So you need to be checking the operating system and the security measures are in place so that Play Protect is on, some of those super admin privileges are disabled. And by doing that you're putting yourself, your data in a much, much safer place. So really, really important to do that. Again, you're going to have to physically access your employee's devices and check this. So again, that might be something that you need to navigate. And if we just go back to those earlier slides, that is why we're saying sometimes you might just go for a lower level Android device with these security features in place and they can access work data that way. You will need to definitely deny the installation of certain applications.

And so you might have a strict allow and deny list. So again, if I just use Grammarly as an example, you might say that's on the deny list. We can't have that because it's logging keystrokes. Other organisations, that is fine. It helps our emails and our content sound much more professional, we're using the right syntax, all that kind of stuff. We're going to allow that. We're going to deny TikTok, we're going to allow Facebook. Whatever it might be, you need to have this so that you can then quickly on a regular audit check, be seeing if any disallowed apps have been installed and at that point, review their employees' bring your own device policy allowance or to restrict it. Once we have that in place, again, these governance standards, we've got to make sure that they're updated and checked. A lot of organisations who deploy a bring your own device will have an initial document and they're like, great, we have a policy.

And then they file it away, not ever understanding that the threat landscape is changing and the employees are changing as well. So we've got to make sure we've got these policies in place and we're broadcasting them to make sure employees are aware of our expectations and that they're compliant with them as well. So we've got a bring your own device initiative, we've got to treat it like a privilege. So employees, if you want to do it, that's fine, but here are some things you must adhere to in order to continue to achieve that. And then the last one, which is always the most difficult, and that is regular audits. So by that, on a monthly basis you need to be checking their devices to ensure that they're compliant with all these policies we've put in place and not jeopardising the organisations, the assets or the data.

And so again, you've got to get your hands physically on this a lot of the times or someone from the IT department just to quickly check that there's no, again, incorrect applications being installed, that there's not company data stored just on the desktop for example. Those sorts of things. Just making sure that there's really sound device hygiene in place because the risks are too great not to.

And then I always ask people to consider this as well. This is absolutely critical. So do we need employees to have access to all this information on their phone all of the time in order to be productive or is it a luxury or something that we convince ourselves that will help us improve the sufficiency and drive client or customer satisfaction? Because it is in some instances a bit of a myth as to what it achieves and what it doesn't achieve.

And so we just need to think about it and go, we really need this to occur because tolls on the road all the time, so we need to be able to access emails and teams versus Tyler's subordinate who's not on the road so much doesn't need that, so there's no phone access for that employee. Just got to be thinking about that and really making sure that it is horses for courses and it suits you well. I can see, again, I know a lot of you are not doing it at the moment and I actually probably support that. I just think it's too big a risk. You should control your hardware at every stage, especially if you're dealing in sensitive information. So we just need to evaluate that every step of the way.

Really what we're thinking about when we use our phones though, there's sort of four key elements. So we've got the instant messaging and this is something that's really gained legs since Covid. Obviously, we're now accessible all the time, but do we need to be using instant messaging on our phones all the time? Probably a lot of organisations that deploy it will say yes because they can reach their employee without sending a text message,

which some people consider an invasion of privacy. One should only do that if they've called in sick or whatever it might be. So instant messaging is a way for employers to contact employees. They can switch it off at certain points. So we're just setting up these effectively, these barriers, these guidelines. But if we're using these on mobile devices, we need to think about the information that we're sharing and the risks that could occur. So real simple rule, we just don't encourage you to share any personal identifiable information on instant messaging and where possible really, really avoid confidential information and delete messages after a certain point.

So there's no point having a massive history because we know most conversations in these platforms are fairly colloquial and not something that we need to go back and rely on as file notes as an example. So getting the information out of there, putting it somewhere safe and then deleting it is one way to safely navigate instant messaging on the devices. Passwords, this is a really tricky one because a lot of people love their passwords on their phone because it provides them that flexibility. They can access all their work assets from their phone, they've got all their passwords with them all the time, but it is often a matter of convenience. Really it doesn't provide any additional security. The authenticator codes are an entirely different beast altogether. But we should think a bit about passwords. So they might choose to keep their personal passwords on their device and that's fine if it's their own device. We should disallow the storing of corporate passwords on a bring your own device especially again, that their use is decentralised and you can't be sure that it's not going to.

They might keep those passwords afterwards and if you're not aware of all of the sign-ons, you may fail to update them. So again, keeping those passwords on a centralised device only is going to be recommended. The authentication, so again, this is the one we're using. Google authenticating apps or Salesforce or Microsoft, whatever it is, those expiring TOTP codes. So they're really popular within while we use our phones to work and help break down that barrier to using a phone for work. And again, the dissection between what's mine and what's works. But again, we say maybe consider a desktop solution for these expiring codes. All of my TOTP codes are stored on standard notes, which is encrypted and so they're all there. I have to fire it up as a separate programme, entirely separate to my password manager and it's all on my desktop.

So my phone, truth be told, I use that dumb phone that is on the screen there initially as my daily driver purely because there's nothing on it that way and everything is stored within the encrypted laptop. And again, most corporate laptops will have BitLocker installed, again, to protect the device that way. So think about that, just thinking outside the square, is the device absolutely critical? What are we using the mobile phone for? Does it have to be on the phone or can we do it with some hardware we control?

And then, the last one is email. I know a lot of people love getting emails, they love responding to emails late at night and it makes the recipient feel that they're very important. But again, we need to consider is this a personal choice or a management directive? A lot of employees like it because they can get to their inbox zero, and I know a lot of people strive for that. But I actually suggest maybe consider disallowing it and make sure you've got really good governance policies in place because you do run the risk of it being a gateway to an attack.

I probably want to show you an example. So let's assume we received this email on our phone at any point, but let's just assume we access it on our phone. So it could be Netflix, could be Office 365, it could be anything. Now in a phishing attempt like this, which is what this email is, this would be much more successful on the phone compared to a workstation, because we do a few things differently. Basically, in our desperation to declutter at inbox, what we really do is we do a couple of things definitely. So we don't check the email address where it's come from because screen real estate on the phone is so important that we never really bother to check it versus on a desktop, we might hover it and notice that it's could be netfli689@gmail.com, but they've just spoofed their address to make it look like Netflix or it may be a little more sophisticated than that, but we just don't do that on the phone. Versus on the computer, like I say, our shields are up that little bit more. On phones, we click that update account.

Now we do it because it's easier to do that than to go into the browser and type the URL, which is what we might do if we're back on our work computer and receive this email because we might be thinking it doesn't seem quite right. And so we would go to, in this instance, netflix.com rather than clicking that red link, which could be effectively a malicious payment gateway, which is exactly what this was. And then we copy and paste our password from password manager, which we probably would do on our desktop. But at the same time, a lot of the times if people are using those browser extensions, it wouldn't autofill because the address isn't correct if you didn't do step two and did click on that link. So we've got these additional security measures in place that come hand in hand with using a laptop or a workstation as opposed to a phone.

And then finally, as it happens often with these malicious emails, we end up in a loop. And so, it'll be saying, oh that password's incorrect, please enter it again and we do it again maybe three times. That's then confirming that they've got the right password so they can then go through and attempt to do your account takeover. So even that happens on that phone, we just put it down to the phone line. These mobile browsers are not as good as my desktop, whatever it might be. And we just dismiss it. Again, when we're at our desk we start to think, wait, something funny is going on here, I might need to check this or I go see my boss or call the IT department, whatever it might be, I think something bad has happened. So this is why we need to really consider that email use on our phones because it holds with it a really significant risk.

And again, these might seem unpopular or that they might not occur frequently, but it only takes one. And we certainly see there's about one to two ransomware cases in Australia per week and they stem from simple emails just like this. And in fact, we're going to go through one. And meanwhile when we start talking about our workstations and laptops, so this is another element that we use for our Bring Your Own Devices, again, a really positive cost saving for organisations and it allows employees to just use a device they're familiar with. Some people like a very fancy computer, some people don't, some people prefer Mac, some people prefer Windows. And depending on where you sit on the browser based work style, you might be able to get away with that. But regardless of the type of device when it is a laptop or a workstation, it's a bring your own device. We lose so much control that we really need to be considering, and this is why it comes back to that really strong governance.

So when it is their own laptop, we don't know who uses it and we can't restrict it because it's not ours. So if I have a bring your own device, I might let my daughter or my son use it. You can't stop me, it's mine. And at the same time, there might not be any appropriate governance documentation say that that shouldn't be done. So all of a sudden they're using it, I'm using it for work purposes and we know what kids and our parents are like when it comes to security on their devices, they're not really great at it. So we don't know who's touched the device, which is a really big risk when it's our own. We can have express rules that say no one else is to use this device.

And generally you would say no, you can't use this as my work computer. Use dad's personal computer. So we've got to control that element. That's a very, very important one. We also think you can't restrict where it's used. If it's not yours, we don't know where it's being plugged in, where it's being taken and those security risks that run with it. So if it is yours, you get to very much granularly control that. You might say you cannot use this at cafes, you can only use it at these locations, and you can restrict it through IP, mapping and allowing as well. So you get some really strong control. When it's not yours, it's difficult to police that. And again, you start telling people what they can and can't deal with their devices and it gets very tricky. So it's something that you need to navigate and make sure that if you are doing a bring your own device policy with laptops and workstations, then this is someone that's trusted.

And again, you've got the appropriate documentation in place. The networks is, again, we will talk about it briefly, but it's something that we've got to be very, very mindful of because with this whole work from anywhere thing, everyone thinks they're being productive and efficient all the time. This is one thing that we're seeing a little bit of a better outcome with at the moment where people are generally not connecting to open networks. So they're not going to cafes and signing in. If anything, if they need to, they're using their hotspot or they're using a dongle

that they've been given. That is the way that they're connecting to networks. And I would have it a guess that given the way this room is with such a heavy slant towards no bring Your own device and again, not knowing what an Android sideload is, which is really positive, they probably have some strong policies in place regarding network usage as well. So that's really, I guess, an assumption but encouraging what we're seeing these days, a lot of people are switched on to this and understand the risks of it.

Side access, this is one thing you simply can't control on a decentralised device. Again, if it is within the work network, you might have certain allowed sites and disallowed sites. So for example, a really common one is any pirating website is disallowed. Almost every organisation disallows that. Social media sites might be disallowed. You can't necessarily control that from a decentralised device. So when it's mine, you can't really control that. And especially if you don't know where I am and what network I'm on, I'll be able to get around that without any great difficulty. So that's something that we've got to really consider in regards to that. And again, this is why bring your own device policy might be best suited, if we go all the way back to one of those earlier polls, in special circumstances where you can really trust the person and make them accountable based on your governance documentation.

And then following on from the site access of course, is the software that's downloaded. If it's their computer, they'll put whatever they want on it. And you hope they're not putting anything malicious on there. But again, accidents happen all the time. So we've got to be thinking about that. They might download malicious software accidentally, which again, the most common one is when people are trying to get their device to be optimised, as a device optimizer is a really common way of delivering malware. So it's free, people download it and then all of a sudden, their files become encryptors of a ransomware payload. So these are things that we've got to be really, really thinking about when we're issuing out a bring your own device. Again, sound governance from the outset will really help you achieve this.

It's probably no surprise here that Windows holds the lion's share of this market space, so 66%. Mac 31, and then Linux and Chrome OS bring up almost the immaterial balances there. So with that, we've got to be thinking about we know that we put a lot of security around our Windows devices, we try and make sure they're safe all the time. Mac is not without its risk as well. And just the other day there was a malware that was able to be deployed to the macOS through a Calendly link invite. So again, we've got to be thinking and have our shields up all the time regardless of the operating system that we're using. But we do know that Windows are where the hackers like to play a lot. Again, it's got such a huge footprint from a workspace perspective, they've got lots of productivity applications, their hardware is readily available from multiple vendors, so it's a little more budget-friendly. And as a result of that we end up with some security risks baked into that.

So much like what with we saw with the phones, you can't go and put macOS on just any device. You can do a hack in to it obviously, but we're not going to get into that generally as Apple's closed off, but again, not without its risk. So we've got to be still making sure we've got really sound policies and procedures in place when we do that. So Windows is the biggest risk, no surprise and it's very easy to effectively make a mistake within Windows. I'm going to show you a second video. We're going to fast-forward a bit and I'll talk over this one. But effectively, I want to illustrate how easy it is for something bad to happen without the employee really perhaps considering it. And again, without our device isolation, we really lose the ability to control this. So effectively, we can assume that this employee has received a file. Vacance_810.doc_.

Now, you'll notice it's got three underscores or two underscores with it. So again, a common way to deliver this is would say for instance, I would say, "Hey Bill, sent you this file. I've had to change the file name extension because sending from a Mac. Just delete those last two and you'll open up on your Word and it'll be fine." Now what we see here at the top right, you can just see don't pay or do pay attention to these, but you would never see these, these are what the processes that's being created in the backend. So things that we don't know when we open a file that's occurring, and this is effectively how a malicious payload is deployed.

So in this instance we can assume the employee has downloaded something from their inbox, might've come from a friend on their own device, and they're going to rename it as would be told to do so simply get rid of the underscores and then open it up in Word, which is what we would all do. And we can see here, so Word's being executed. There's nothing in the file so we just think, oh, something's wrong there. I should pop in the password that we have been provided.

And so, as far as we can see, nothing's really happening but what we can see here is there was some executable files dropped into this system here. So we'll see if I can go back to make them a bit broader. So we can see in the app data files, there's been a couple of applications dropped from there and we also now start to see a lot of activity in the background. So as that application was closed, now there should be nothing happening. But here we can see we are starting to see some activity occur in regards to that malicious file. So you'll be going about your business after opening this file, you might jump back into your inbox to email back bill. Then you'll say, "That file didn't really work, can you send it to me again please?" But again, what is really happening is... I'll just scrub ahead here.

So we can see here that we've got some child processes created within the route directory, the system directory, and then all of a sudden our files are encrypted and we've got no ability to access any of the files within our desktop. And what happens as well is if we have company data on here, it's potentially synced back up. So that poses a really significant risk from an employee perspective and employer perspective, which is what we need to consider with our Bring Your Own Devices. It is a big risk. So we can analyses this, a few things that went wrong with that example. I appreciate it'll happened a bit quick. But more or less that's how ransomware is deployed. It can be something that looks as innocent as a document or a spreadsheet or an image. And within that it is containing malware. So we saw that there was some poor governance at play here in that the employee was able to download a file from perhaps someone that they don't know or that they do know on a mixed-use device and then effectively open that.

And so this is where we've got the problem is when personal is crossing over with company. There's no virus scan on the file and Windows didn't automatically do a virus scan. So these are things that you can control with your own organisational devices, constantly scanning files even before they're downloaded a lot of the time. But certainly, once they are downloaded you might say you need to scan this for viruses, and ideally that would've been picked up at that point. This user had admin privileges. Why not? Because it's their computer. So they were able to instal applications. Now they didn't instal it, the malware did itself. But again, if they were just a standard user that may have run into a brick wall at that point and not been able to access the admin privileges to effect for that ransomware to deploy, and at the end their computer was completely pwned and all their data was lost.

And at the same time as we've seen with ransomware these days, that will be then exfiltrating that information and then also potentially extorting you, all leaking sensitive information out. So this is just something that we need to navigate and be really careful of. So how it could look different if we used our own devices more or less? So we would have better policies and procedures, wouldn't we? So we would have a much higher level of control in regards to what can be downloaded, what what's allowed to be accessed. And generally, you might assume personal emails wouldn't be accessed on a work device and therefore, if that file was malicious, it could have come from a trusted source within the organisation and the employee might feel a little bit better about that. We would then also make sure that... Sorry.

There is download controls. So again, you might not be able to download files. Again, there'd be virus scanned at the outset. Again, really restricting that. You might not be able to rename the extensions as well. Again, so you can really set these granular user controls down. It's really important to do that. Again, user privilege only. So there's no reason for an employee to ever have admin privilege on a work computer. They shouldn't be installing things, they shouldn't have the ability to instal things. And these are things that you can restrict when it's your own device. And then also, you'll get alerts and updates. So whether or not you've got an intrusion detection

system or not, you might get alerts that something was trying to send out of band traffic, for instance, it may have been trying to call to a server located in a strange location.

You'll get these sort of alerts. Your IT department, your cyber security department, even just your IT champion might be able to come in the next day and say, "Did you know that Tyler's computer was doing something really funny last night?" And all of a sudden you potentially can stop an attack before it really goes any further. So that's something that we need to consider in regards to Bring Your Own Devices and workstations because they do pose a pretty significant risk. And then finally, I'll talk about network access and I'll probably try a little bit to get through still, we're running out of time. What happens, what we don't think about this is that our devices, all of them are constantly broadcasting, looking for a network to join. And so when it's a private device, there's often a lot more that it'll be searching for.

So you might've gone to a cafe at one point with your own phone, used that, and then you've also used it at work and joined that wifi. Again, not necessarily choose huge risk there, but what's happening is that it is constantly looking for these networks. So when it's our own device, we can restrict network... When it's an employer device, we can restrict network access and we can also forget the networks that we don't want them to be, remembering because we are controlling it from this centralised location. Again, you can deploy devices, Apple as an example from iTunes, so you're controlling all these devices from one location. Again, these open networks are really big risks and what I've really shown you there is just some devices that I use when we're on engagement, and we use these networks as a wave to get a foothold, so to speak.

So if I had those plugged into my computer, which I do, you might not think there's anything funny going on, they just look like a wifi router really, or a modem. And we use those in order to get this network information, which then we're able to effectively piggyback on and leapfrog across. The reason that this is a risk is because most households have about 15 to 17 devices connected to a network at any given point in time. So that's a lot. And that means that we are also asking our employees to ensure that all these devices are secure as well. It only takes one insecure device. So when we trust them with their own network, we're actually saying effectively you need to ensure that all your devices are safe. And again, if you think about your children, your parents, your internet things, devices, can you guarantee that not doing anything that could compromise your network and therefore potentially compromise your work device.

So huge risks, one that we don't think about because we're just happy that they've got internet and they're away. If you can, again, start thinking about deploying a centralised network, take this dongle. That's the only way you can access the work data. And again, virtual private networks are a really big help as well. But the networking thing is, again, because it's not tangible, it's sometimes something we don't think hard enough about and we really, really need to because again, it's very easy to leapfrog across. And then if that employee's device is not secure, potentially your organization's data is no longer secure as well. So we really got... We know we've got some significant challenges when we're talking about bringing your own devices. We've got cost, it's expensive if we're supplying every employee with phones and computers, and that's why I implore you to consider do they need to be mobile all the time or is it just occasionally?

But that will help you eliminate some of that risk if you're not having to get them phones or computers. And again, also eliminate some user risk. Speaking of user risk, we know employees, people are much more careful with their own stuff versus other people's. And so, your phones and computers as the employer are no different in that instance. So that is why Bring Your Own Devices is a little more popular and encourages sort of an investment from the employee in that regards. We have environmental considerations as well. E-waste is significant, so it helps us minimise those impacts, which is something that's very real and something we do need to consider. And then we've got a really high employee throughput at the moment as well, which means devices are bouncing around everywhere. Asset management has become arguably a full-time job for some organisations. So when they've just got their own, it just makes life that touch easier.

So just depending on where you sit on the side of the bring-your-own-device spectrum, there's a few things that we need to make sure that we take away from this. So if you are yes for bring-your-own-devices, then you really need to make sure that you've got some strong internal governance. And I would encourage you to pause your bring-your-own-device policies until you've got this in place because it is going to be a lifesaver if something ever happened. So having that, don't issue out a bring-your-own-device without employee endorsement of this governance as well. You need the data isolation. And by that, more or less, you can't store company data on your personal assets. It should be just that. They might be able to access it, but you need to come up with means to make sure they can't download it, save it, and therefore put it at risk.

And again, VPNs are a really popular way of achieving this, but we need to make sure they can't just save it to their personal desktop, which again, a lot of these remote desktop protocols for those that are still using NOs, some of these cloud solutions, you simply can just download it. So we've just got to be thinking about that. How do we protect our data that way? And then finally, checks and balances. So it's all well and good to sit here and say that we've got a governance policy in place. I said we have to regularly be getting our hands on the devices and checking them. That is the biggest challenge because employees will not like that. I personally wouldn't like it. And I've got such a problem with it, maybe I won't do a bring your own device. And if you really want me to be accessible all the time, maybe you'll give me a device then.

So again, we start to see the motives of the employer and the employee, and by doing that we then really increase the overall security for that. If bring-your-own-device is not for you based on what we've discussed here today, you do get a lot of device control, as we said. We get that granular control over the entire device, what can be installed, where they can go, what they can do. And not trying to turn your workplace into a police state, but it is about making sure that the device is used for a deliberate purpose. So again, if they want to muck around and go to Facebook, yep, fire up your own computer, we don't care. Not on our device. Whatever it might be. So again, we're not, again, not trying to make it seem like employees are up to no good, or it is simply about cybersecurity.

You can reuse these devices. I just don't understand why people think that they have to throw away a computer when someone leaves. Simply securely wipe the hard drive and then reinstall the operating system and it's good to go. You just don't need huge amounts of RAM storage these days in order to do your work effectively. And like I said, short of the device being physically damaged, there's no reason that you can't reuse these devices. So I really do encourage you to get in the habit and the mindset of doing that. Safely sanitise them and then redeploy them. And when you do disallow Bring Your Own Devices, you still need governance. So it's really important that employees have a really sound understanding of what they can and cannot do on employer hardware. Where they can use it, where they can't, all that stuff should still be documented and broadcast to them to make sure that there is an awareness and understanding.

So through all of this, what we want is employers and employees to be on the same page from a cybersecurity perspective and ensuring that the data is never put at risk or compromised because that is, ultimately the whole purpose of this is to protect the data and still drive business efficiencies. So again, this is why some people will vote for Bring Your Own Devices and we'll deploy it and others won't. And again, it is very much horse of the courses. So we can achieve both. We've just got to make sure that we've got them again, a plan and being deliberate, the actions to achieve both. I'll hand back to Susanna to wrap up in case there's any questions, but I hope this has given you a good understanding of Bring Your Own Devices, the risks and challenges and just some simple solutions that we can deploy to make sure that we are all safe online.

CCH Learning:

Thank you very much for that, Tyler. That was great. Yes, we will be spending the next few minutes taking questions. So please type them into the questions pane. To give you some time to type those up, I will mention our upcoming webinars. So coming up, we've got how to best extract funds when selling a business. We'll also be considering aged care with couples care and considerations. We have an income tax update case, income tax case update coming up, and also non-commercial loss rules for individuals. We'll be looking at the ins and outs of Super and a broad look at contributions and pensions.

The 13th of March will be the next in our FBT 2024 series with understanding entertainment and meals. If you're interested in these or any of our sessions, please head to CCH Learning website, have a look and see what is right for you. So let's have a little look at our questions. So I have a question here from Mark. Mark was asking, "How do we go about getting employees to actively share their phone installation activity with the organisation? But could this be an invasion of privacy? I wouldn't want someone else handling my phone."

Tyler Wise:

Yeah, that's probably the biggest risk you've got. So at the outset, before you let them access the data, I guess probably explain to them again, have that documentation that says this is our policies and say on the monthly or however it might be, we need to sit down together and go through the device and inspect what's being installed. And if they don't like it, again, I personally wouldn't like it myself, but then maybe it'll help me decide do they need access to the information or do we give them a device of their own or they might be open to it. But yeah, it's a very tricky one to navigate and just handle it delicately and you'll be fine.

CCH Learning:

Thank you very much for that, Tyler. I hope that helps you there, Mark. I also have a question from Sarah. Sarah was asking, "Is there a risk that an employee will simply just uninstall everything in advance of a phone or computer to company audit?"

Tyler Wise:

Yeah. Yep. There is. And there's no real way of knowing that or policing that. You could do random ones, but all of a sudden I think that that just gets employees completely offside. It's hard because you would be... There's probably no real way around that because if you have suspicion of it, you might have suspicion of other things, in which case you probably relinquish their bring-your-own-device control. And you could look at imaging the entire device, but again, starting to get really technical now and probably defeats what you're trying to achieve with the bring-your-own-devices. So yeah, again, those strong governance protocols. And then if you're suspicious of that, I would just relinquish their ability to use the bring-your-own-devices because they're obviously not doing it in the appropriate manner. So if you're feeling suspicious about anything, I would say probably act on it. But as far as being able to check if they've done it, short of engaging a digital forensic expert, no real way sitting opposite the employee.

CCH Learning:

Thank you very much for that, Tyler, and I hope that helps you there, Sarah. Well, that does seem to bring us to the end of our questions for today, but if you do have further questions, Tyler's details are there on the screen, so please reach out and I'm sure that Tyler would be able to help you.

So in terms of next steps, I would like to remind you all to please take a moment to provide your feedback when exiting. We've asked you a couple of questions about today's webinar, so it's really important for us to hear your opinions. It's also a reminder that shortly after today's session you will be emailed when you're enrolled into the e-learning recording, which can be watched multiple times. And of course, you have access to the PowerPoint transcript and a CPD certificate. I would very much like to thank Tyler for the session today, and to you, the audience for joining us. We hope to see you back online for another CCH Learning webinar very soon. Please enjoy the rest of your day. Thank you very much.

Tyler Wise:

Thanks.