Microsoft 365 Security- Is Your Organization's Data Safe

Microsoft 365 came of age just as organizations quickly adopted remote work during the pandemic. In their urgency to migrate, many IT departments did not have the time to fully research the new platform and all its security features, opting to use the default settings. Once migration was complete and systems running reliably, organizations — fearing disruption — may not have gone back to change the settings.

If your organization uses Microsoft 365 products (Outlook, Teams, Word, Excel, OneNote, OneDrive) you will want to watch this complimentary webinar. We discuss the underlying default security issues that exist and what you need to understand to make your Microsoft 365 environment safer.

Find additional resources on our event page: https://www.claconnect.com/en/events/2022/is-your-organizations-data-safe

Here is a transcription of this session:

David Sun: Good morning everybody or afternoon, depending on what time zone you're in. Thank you so much for joining us today. We appreciate your interest in the Microsoft 365 security webinar here, talking about whether your organization's data is safe or not. A couple of quick things, real quick to get started. We got a slide here with some disclaimers and notices, so I'll throw that up there. And then what we'll do is go ahead and do some introductions for your speakers for today. My name is David Sun, I'm a principal at CLA and I lead the cyber incident response and forensics practice here. Let me hand that over to our next presenter, Dave Hale to introduce himself.

Dave Hale: All right, thanks David. Hi, I'm Dave. I'm in the CLA digital group, a director there and have worked for 10 plus years doing Microsoft 365 from even back in the BPAs days doing everything from migrations to set up, training, support. So very familiar with the product stack here. Nehemiah.

Nehemiah Jones: Perfect. Hello all. My name is Nehemiah Jones and I work directly with David Sun on our IR and forensic team. Unfortunately a lot of those involve Microsoft 365 compromises, business email, et cetera. And I also perform a lot of our Microsoft security review work.

David Sun: Great. Thank you all. Thanks for joining us today and thank you everybody for joining us. This is a very well attended webinar. It appears that we have over 1,400 participants here with us today. And so really grateful and appreciative for everybody's interest. It's a hot topic, right? Because Microsoft 365, it's a great platform. A lot of organizations are using it. It's got lots of great features with email and calendar and Teams with messaging and OneDrive and SharePoint. It's a very feature rich platform. CLA uses it. And it's quite popular out there. As it turns out it's sort of got the majority share here as a February, 2002, so eight months ago it's got 47, 48% of the market share in terms of cloud enterprise, cloud platforms.

So again, a lot of people are using, a lot of organizations that are using it. And the thing is, it's great and it's got lots of security features and everybody's using it, like I said, but guess what, it means

the hackers also know that everybody's using it. And it's one of those things where if you're a hacker and if you're a bad person and you want to identify and create and invent ways to compromise systems, you're going to go after the systems that are the most prevalent. You're going to go after systems where if you identify one vulnerability, one hack, one way of doing something, it's going to work for as many organizations as possible. And that's where we are with Microsoft 365. Because of it's popularly in prevalence it's become a big target.

It's actually what I would say is one of the most compromised cloud platforms out there. I talk to a lot of clients and they ask me about cloud platforms, I tell them that Office 365 is great and that CLA uses it. I tell them, by the way, it's the most compromised cloud platform. And the clients always say, well, we just got compromised, David, why are you telling me to go to another platform that's so often compromised? I have to explain to them it's actually a good platform. There's a lot of wonderful security features that Microsoft has built into the platform, over 120 different security features and settings. The problem though, the problem is that for whatever reason, and I don't know why they did this over at Microsoft, but a lot of the security features that they created on the platform, they're disabled by default.

I suspect it might be because of ease of migration, ease of use, convenience, make it a smooth transition and things like that. Because as we all know, security inherently means inconvenience. If you're securing something, you're trying to keep hackers out and chances are you're also going to keep your own people out or cause problems with your own people as a result. And so I think that's maybe part of what happened. They disabled a lot of those wonderful security features by default or in the case of something like legacy authentication, that's a feature they enabled by default, which is unfortunate because that's a source of a lot of compromises.

What we found out there is that, I'm just making general statements not directed to anybody or any organization in mind, but what we've found is that a lot of the IT administrators out there and your managed service providers, the people who are out there doing sort of day-to-day operational upkeep, keeping things running, with Microsoft 365 being fairly new, we find that most IT organizations and most IT administrators know maybe 10, 15 of those controls roughly out of the 120. And that's what they're familiar with, what they're comfortable with. And unfortunately because Microsoft 365 is new, they don't have the familiarity. They haven't had the time to research and learn and understand all the different security features that are out there.

And so as a result they don't know what to do with them. And so here's your typical Office 365 migration that we see a lot of. We see where IT understands that set of 10 to 15 security controls and they know to implement those, whether that's multifactor authentication, maybe they're doing some conditional access settings, they're doing spam filtering. But the problem is that they don't have the time, resource, energy, budget, whatever you want to call it, to really dig in and understand all of those, do that deep dive. And so they know that the 10 or so, 10 or 15, they hit those, but the rest of them, they just let it go and they use the default. And as the migration deadline approach, IT starts getting into a rush.

Again, their job, IT operations job is to make sure things are up and running. So when they're doing a migration, their primary focus to make sure that email and documents are migrated to the cloud, that nothing is lost and that you have minimal or no downtime as part of that migration. Those are the things that IT is focused on when they're doing their Office 365 migrations. Don't lose the data, don't have an outage. And so they're unfortunately not able to spend the time needed to really get into

the security aspects of things. The other thing we're also seeing is we're seeing that it's very, very uncommon for IT organizations to do a security assessment or security review of the office their Office 365, Microsoft 365 environment before they do the migration. It's the old, well, I don't have any data in there. What do I have to worry about securing?

And I get it, I understand that line of thinking, but the problem is once you finish your migration and all your data's in it and you've gone through that horrible IT week of stress and anxiety of doing the migration and you're successful, what's the first thing people want to do? Is it getting in there and changing the security settings that might cause email to now stop? No. They want to sit back and maybe have a drink and relax, catch up on some sleep. And so after the migration is over, IT is not thinking about how do I make this more secure? No. They don't want to break anything. Email is working, don't touch it. Let's move on. I got another project that I'm falling behind schedule on. And again, that's your typical IT scenario that goes on.

And so we see the unfortunate consequences of this. My organization, Nehemiah is on my team, I have others on my team, we do numerous incidents that we respond to and there's always one that we have on our plate that is caused by a business email compromise out of Office 365. That's where hackers got into Office 365. They accessed people's email and they're doing bad things as a result of having accessed that email. Wire fraud is a common one where they hacked the CFO's email account and they're sending an email to the bookkeeper or the account's payable saying, hey, please set up this vendor. Please wire, please pay this invoice. We have one on our desk right now where the client lost $2.4 million, and this is a client that cannot afford to lose $2.4 million. It's very unfortunate, but it's a very typical Office 365, Microsoft 365 email compromise.

We see them all the time. We've seen them for years. What's happening? How are the hackers doing this? Right? Well, they get in there, they figure out credentials. How are they figuring out credentials? Maybe they're sending out, they are doing it through a phishing email. Maybe a user has used an old credential, an old username, password that was part of some other hack somewhere else and so it's floating around the dark web. Who knows? There's tons of ways for people to figure out somebody's username and password. And then with that username and password, they're logging into the Outlook web access, that web interface of Office 365 and then get in because my multifactor authentication is not enabled. That's the first problem. If you don't enable multifactor authentication, they're getting in, they're going through the front door.

Maybe they're going into the back door, the side door, they're using an old email client, POP, Eudora, anybody remembers that? Or some type of other old email client and they're using something called legacy authentication. That's the back door where even if you have multifactor authentication enabled and enforced, if your IT department missed this one, if they didn't disable legacy authentication, they've kept a backdoor open. And it's ironic, right? Because basically IT groups spend so much time and energy to implement multifactor authentication and the inconvenience to the user base and they've left the backdoor completely open for the hackers. It's kind like the worst of both worlds where the users got inconvenience but the hackers got in no problem.

Let me say authentications is a huge thing. And then what happens is we see the hackers come in and they log in and they access email and we see them accessing the inboxes from strange IP address in Germany or in North Korea or something like that. This is an example where the IT organization maybe didn't implement the geofencing features that are in Office 365, which would prevent users from logging in from strange IP addresses or strange countries. We've actually seen lately where as

multifactor authentication is getting more present, we are also seeing hackers being able to bypass multifactor authentication. And how do they do that? They spam or they prompt the user and the user for whatever reasons decides to hit the okay button on the multifactor authentication app. And that's horrible.

We've also seen other men in the middle type of attacks going on where people give up their six digit code inadvertently. It happens. So the point being that multifactor authentication, it's not iron clad, it's not going to ensure that you're safe, but it adds another layer, it makes it harder for the hackers. It's good to do it. But again don't think that just because you have MFA, that you can go crazy and let your shields down. What else goes happens during compromise? They forward emails, they create these email forwarding rules, they redirect emails. Again, they're doing the wire fraud where they're sending emails to maybe one of your clients saying, hey, we're following up on unpaid invoice, we've changed our banking information. So please update your wire information and send payment for this invoice to this new place.

They'll create rules so that when those clients respond saying, yep, took care of it, no problem. Those emails don't go to the CFO's inbox, but they get diverted somewhere else and the CFO doesn't notice something's wrong. Again, what I've showed you here on this slide is your typical business email compromise and we see them all the time and we see hundreds, thousands, millions of dollars being lost as a result of these compromise. And so what is happening? Right? Well, what is Microsoft doing or not doing? And then again, I don't want to put the blame on Microsoft, that's not what I'm trying to do. But why is it that in this Microsoft environment that these things can happen?

Well, there's a couple of things. There's a little licensing maze, which is really complicated licensing that's out there and it's hard for people to understand what license they need to get, which features they want. And we'll go over these in a little more detail here. There's the dangers of the default configuration. I mentioned the default fault configuration is not a great configuration. It works, but it's not very secure. Talk about IT overload, IT admins are trying to figure this out, trying to make this happen, but they still have the resources. And then regardless of those things, there's just the general risk of cyber threats that's always out there. So with that, let me turn this over and we'll dive a little deeper into some of the big reasons that are going on, so that everybody understands what's really going on. Let me hand this it over to Dave Hale.

Dave Hale: All right, thanks David. As David mentioned with the licensing, I really wish we could stick to corn mazes and not have to deal with licensing mazes, but we're here with, have to handle that with Microsoft. Now, talking about Microsoft's integrate security, they really do have a great story to tell. From Microsoft's perspective there's a lot of great features that Microsoft has from identity access management. If you want to configure single sign-on for all your applications through Azure AD, you can do that with Microsoft. If you want threat protection, if you want to have safe attachment policies, safe link policies in your email, you can do that.

Information protection, if you need to send secure emails, if you need to encrypt documents and be able to protect the information at the file level, that's all capable within the Microsoft stack. And even security management, you can take advantage of things like defender for cloud apps for visibility into your third party app, cloud apps that you're working with. You can use something like Azure Sentinel for monitoring to bring it all together. There's really, really a lot of good features Microsoft has. They have a great platform to back it on with the billions of signals that they take in every day, analyzing

the data from the threats at their data center level to even the individual devices. Because you can add on defender for endpoint for antivirus, and we can monitor all of that.

So Microsoft really has a good story to tell here at it, but you do fall into that, well if I want to take advantage of all of these features, how do I do that? And that's where you can run into the trap here of this licensing maze that we call it, where Microsoft has individual plans based on, do you need plan one or plan two, so to speak. And then they have bundle plans here. So as an example, there's over 400 individual service plans that are out there for what you need. And they do have bundles that include a whole bunch of those security features that I mentioned. The E5 plans have them. Even something like business premium, if we take that as an example. Microsoft Business Premium is a great plan, but a lot of organizations may be running something like Business Basic or you may have Business Standard.

That gives you your email out of the box, it gives you SharePoint, gives you Teams, OneDrive, really great collaborative features. But what if you wanted to have conditional multifactor authentication? You know what, I only want to require MFA when I'm in the office or when I'm outside of the office. When I'm in the office it's a safe network. What if you want to be able to send encrypted emails? Well with Business Basic, Business standard, out of the box you're not going to get that unless you add on certain features. Something like Azure Information Protection for encryption or Azure AD Premium to help you with conditional access policies.

All those add-ons get added in and until you're at a point where you have to decide is am I just adding on and buying products willy-nilly or do you bundle in those products into a bundle. And you step up to a business premium or the Microsoft 365, the E3, E5 plans and so forth. I give credit for Microsoft for having all of this flexibility and features, but it can just get a little overwhelming at times. And to tack on here, let's take a look at another example. What if for keeping your data safe, you want to look at retention labeling. Everybody wants to set policies such as you might want to hold onto your email or your documents for a year, maybe 10 years or indefinitely, depending on your organization. And you can absolutely do that with the Microsoft platform.

There's things, Microsoft Purview, used to be called information governance. Now it's called Purview, data life cycle management and things. And you can do labeling, you can do manual labels on folders, you can do automatic labeling and things and you can get really granular and have that control over retention labeling. But how do you license for that? Right? Because it's not so simple out of the gate, it's not just a one plan retention add-on. You actually have to break up the Microsoft tenant into a couple different products. If you take Exchange as an example, what you may not realize is Exchange online comes in multiple flavors. There's plan one and plan two. Plan one gives you a 50 gig mailbox. Plan two gives you 100 gig mailbox plus archiving and all sorts of other things that, retention and things like that.

If you're on as an example, the business basic or business standard plan, you're not getting the retention right out of the gate with that unless you do some sort of add-ons or you bundle in and take on a business premium plan. SharePoint, if you need to go to SharePoint plan two to do some document retention. Teams as well, depending on the different features, you can get even more granular. There's adaptive scope. If you needed to control a certain group of users in one country versus another, you can have various retention policies applied to it. But it really depends on the licensing net you have. And you can just see here, there's E5, there's A5, E3, it can just get a little overwhelming again that you have that.

So the moral of the story here is really take a look at those licensing, understand which ones do support that cross application retention policies. So maybe if you are on something like Business Basic or you only on exchange only plans, the plan one, you might want to think about the business premium or the Microsoft 365 plans to get you that governance and protection on your documents and emails. And really, as I mentioned, and I'll stress it again too, that it is overwhelming and that it can also be difficult to talk to the CFO, the executives in here, to increase the spend of the licenses when you say you already have a mailbox, but why do I need these extra things? Well, retention is one of a really important aspect of keeping your data safe, especially from, as David mentioned, with the hackers that can compromise your systems.

And if you don't have the proper retention in place, things could get lost. At CLA we do have a spreadsheet too that we cover each individual feature in a list here and it's over 2,400 rows, just showing how much configuration and changes there are. And there's websites out there that you can go to where you can review the various bundles and Microsoft does have thorough documentation as well, but it can be a little overwhelming there to be able to find all of that. It's just so, so critical and important that you optimize your license. So number one, that you are configuring the tenant for the proper security that you need, and two that you're not overpaying for licenses. If you're not adding on all these individual licenses like the business standard, adding on Azure AD premium, information protection and you're well into the 20, $30 range where business premium, I think it's $22 for business premium.

So you can save money too. If you license and price it right you can have a secure tenant once it's configured properly. All right. And so getting into that configuration and having that, so what do you get out of the box there? I think Nehemiah will talk a little bit about that danger of the default config as you all do it.

David Sun: Real quick, let me interrupt because we're getting some good questions here and we're going to get to them. We'll have time, sometime Q&A. But there's one question that I see here that it's timely, right? So let me ask you Dave Hale. The question was, are the security features additional costs or included with the subscription?

Dave Hale: It depends, right? Some of the security it's baked in with Microsoft that you can selectively enforce MFA. Business basic, sure, you can pick and choose users to do that, but a lot of that advanced policies we talked about, conditional access policies, those require a higher up plan such as Azure AD Premium, Business Premium and so forth.

David Sun: Great. And another question again on the licensing plan. We're currently on the non-profit E1 plan and need to be able to download the Office 365 office suite. Is there an add-on option that gives us that ability?

Dave Hale: You can certainly add-on the office apps for it, but I would also think about do you need to upgrade to something like the E3 plan? So for non-profits you can jump to E3 and that includes at a discounted price, the Microsoft Office app. I would look at that because there is a nonprofit price for the E3 plan.

David Sun: All right, great. We'll take a pause on the QA. We'll get some more content and we'll come back to QA later.

Dave Hale: Okay. Great.

Nehemiah Jones: Awesome, awesome. So reason too we're really focusing on the default config and assuming that you have all the security features enabled. I know Dave and I, we've talked about it with the licensing maze. A lot of our compromises are because people they don't pay for their licensing because they don't value security. But there's another danger in trusting the default config. Just some examples off the top, Microsoft has a history of promoting and Dave talked about this, features over security. Listen, Microsoft's an office productivity, business productivity company. They're selling you email services that work. And a lot of times, even though they have these security features in place or they're working on them, that doesn't take priority over just keeping people email flowing, keeping the features, keeping those collaboration features and platforms in place and working.

A couple of examples that are actually in the past are being phased out. Legacy authentication. Dave talked about this. This was the bane of business email compromises, old legacy protocols that couldn't use MFA, and Microsoft said, hey, we want your stuff to work, so we're just going to let it bypass. To give you an idea of the scope, when we used to get calls like, hey, we have an issue, somebody's email, there's a wire fraud, we're in 365. Two questions we used to ask people, is MFA turned on? And a lot of people, especially recently, yeah, we have MFA. And then two, let me guess, legacy authentication was still enabled. It was like we didn't even need that much explanation, you could just literally get a phone call and guess exactly what happened.

But finally Microsoft putting the hammer down saying, all right, end of October we're turning it off or starting to turn it off for basically everyone. Like I mentioned, it was really one of the biggest issues in business email compromises for years and it just festered there. And it's a good example, I know it's going away, so next month hopefully it isn't an issue for anybody. But it's an example of the Microsoft issues with the platform and that default config. Another example was auto forwarding. This was classic data exfiltration. It's basically someone already got access to a mailbox and they begin to redirect email messages. It's a whole lot easier for the hackers to get a stream of emails in the one inbox, then they're constantly having to reauthenticate the 500 inboxes that they've compromised.

And it used to be turned on by default. You used to be able to just set up a rule, forward it to anybody's Gmail, Hotmail, Proton Mail, whatever they wanted to send it to, and start forwarding your emails right outside of the company. And as far as the end user was concerned, they didn't see anything, they still got their messages, everything seemed fine. And then once again, this was originally turned on by default. Let's get into some areas where there's still an issue. These were issues in the past. Let's talk about current default config issues. One of my favorites is, I call it the cascade of terribleness. It's the share settings in Microsoft 365. Once again, it's a collaboration platform.

So Microsoft makes your collaboration easy, but from a securities perspective, the default share settings are a disaster. First off, anonymous links, this one really doesn't need that much explanation. You're able to create an anonymous link that never expires. I was working on a business email compromise just the other day, unrelated, I was going through activity, looking at some logins from foreign countries and stuff and taking a broad view and I saw some sharing in the Philippines, what is this? It was months before our compromise. So it really wasn't that much in scope. And come to find out there was an anonymous link to some company files and somebody in the Philippines found the link and has been accessing it for a couple months.

When people create links, they don't expect it to persist for a year or two years, but that's the default config. But let's say a lot of companies understand the risk of anonymous links and so they turn it off. And they think, well now I'm safe. Now I have control over what's going on. And unfortunately

that's not the case. This is where the cascade of terribleness comes in. There's a whole series of features that chain together that basically mean you don't have much control in the default config or any control really over where things get shared. All right, so what are those features? First off, by default, any user can invite any external party as a guest, right? All right, so now you have a guest that could be from anywhere and they can share files with that guest. Okay, great.

But the key thing here is that guest by the default can also share anything they have access to, to anyone they want. It's not just the guest created document, they uploaded it, it's their document so of course they can share it whoever they want. They don't even have to create the file. Just because they have access to it by default, they can just share it off to whoever else they want. That's a disaster. That in the combination basically means even if you turn it off, anonymous links, if you haven't configured these settings correctly, you still might not have any control over where your information is going.

David Sun: Nehemiah, to put a point on that, basically what you're saying is if I have a document and you are my guest, and I share that document to you, you have access to it. But unfortunately what I can't control is if you go and share it to your friends and your friends share it to their friends and so on and so on, and 10 degrees of separation later, there's people I had no idea was accessing that one link that I share to you. Is that what we're saying?

Nehemiah Jones: That's exactly what we're saying here. And keep in mind the controls are there, they're just not enabled. Microsoft gives you very granular and you can see this page, there are so many different places you can go to restrict it, but it gets overwhelming. You can go and you can restrict it for SharePoint. Those settings are separate than the ones for OneDrive. Then there's guest user access, there's collaboration settings, there's Microsoft group and group owners rights configurations. You can see there's four or five, six places you got to go, and you can use that to be very granular, but it also can be confusing. And we also see a lot of times where, like we talked about an IT person knows maybe one, maybe two, and they leave things open because they don't understand the configuration or they think that there's somehow a secure baseline that they're getting.

And next really focusing on those features again, even if you have to allow a guest, like listen, we're in a collaborative business environment, there's oftentimes you're going to have to allow some level of guest access to your tenant, right now you can turn off them sharing things and cut that off at its knees. But they still need a lot of times for people to have guests. But Microsoft provides ways to monitor that, to review that, to grant access, all these great features. But once again, they're not going to be enabled by default, either A, because of your licensing, or B, because you have to go in there and set it up. I think there's a lot of people, and I'll mention it again at the bottom, who want to always point at Microsoft for the problem.

But the issue is Microsoft can't predict what you and your environment needs. They can't tell you who you're going to have to share information for your business purposes. It requires somebody who understands your environment, who understands the features and controls, and then you can use it. Microsoft can't just willy-nilly enable all these great security features because essentially their system wouldn't work for you. All right, so onto another one that's very concerned.

David Sun: Before we move on from your cascade of terribleness, we got a question that goes right here. The question was, can they share more than the file they have shared? Do they get access to other folders and files?

Nehemiah Jones: Sure. They're not going to be able to just grant themselves access to a folder that they don't already have access to. So for example, if you added them to let's just say a team, like an HR team, they're not able to then go access the finance team and share that out. But anything in that team that they have access to or folder or whatever, however you shared it to them, they can share stuff out of there, if that makes sense. So anything they currently have access to, they can share out, but they can't start granting themselves access to things that you haven't on the back end.

David Sun: Great. All right, let's go on.

Nehemiah Jones: Let's go on. So SharePoint infected files. So Microsoft 365 Defender has a feature, it scans your SharePoint for infected files. Now this is an advanced licensing feature because you have SharePoint plan one does not mean you have this, okay? But if you paid for it, you have Windows Defender have this advanced security settings, great. The problem is it doesn't actually prevent people from doing it. It'll warn them, it's like, hey, we don't like this file, but they can still download it, they can still share it by default. It's like if you say you're antivirus to just tell people, yeah, this was bad, but allow them to do whatever they want to do anyways. It's a disaster.

And this one's even hidden, you can't even find it on the portal. You have to go in the PowerShell, you can see that at the bottom. But it's another one of those confounding things where Microsoft's like, well I don't want to stop people from working. And I can give you an example. I had this happen to me with the setting enabled. And I was trying to get ahold of IT, infuriated, come on, I can't get to my file. I know this is a good file. It's frustrating from a user perspective, but the security issue is still there behind it. PowerShell and admin portal access. Here's another great example. I bet most of the people on this call don't even know what I'm talking about right now, and that's the point. Standard users really don't have any reason to be accessing the Azure admin portal or running around with PowerShell. It's not useful to them.

They probably don't even know how to do it. But there's a ton of information that a hacker can gain by using these tools. And they're the ones attacking your environment, you better believe they know these things exist even if your users don't. You can go in there, you can enumerate all your users and groups, see who's in your admin group, see who's in your finance group, all those different things. They can view many of your security configurations and say, okay, look, this is enabled, this is not enabled, and see how to further attack your environment. They can't gain a ton of valuable information using these tools that Microsoft has enabled by default. As well as with PowerShell they're able to run scripts by default and have all their attacks automated.

These are things that there are sometimes business reasons why something like PowerShell needs to be enabled. I always warn people when I advise them, like listen, make sure you're not using an app that uses it. But most organizations aren't, and most of the time it's much more of a risk than it is actually helping your organization. But by default all this is turned on. So summarizing what we're saying, I want to focus on what the default config is not. The default config is not Microsoft's recommendations for securing your environment. We talked about this a bit above. Microsoft cannot predict what your business needs and they're also incentivized to make their collaboration tools work. So they're going to promote a baseline level of security that they feel like everyone can pretty much implement and then they're going to let it go from there.

Like we said, Microsoft's obviously going to recommend you put in all these security configurations, use all their tools, lock it down if you can, but that they can't enable that by default. It's

also not a highly secure configuration, you just need a couple little tweaks. We saw some examples today and there are some even bigger ones. I'm telling you right now if you have an external spam filter, there are some controls in 365 that just have to be configured. It's technical and not right for this audience or presentation. But there are some big deal issues. I hear phrases like this all the time when I'm dealing in IRS, the one that I have here on the side or dealing with just general IT admin stuff, they say we use the default since that's Microsoft security recommendation and they know more than I do and they understand their platform and that's just wrong.

Almost every single IT environment is going to need some level of configuration, some level of customization to increase their security from the default config. And just emphasizing it's not all Microsoft's fault, they can't predict your business needs, they don't know your implementation strategies. They provided you a platform of tools and given you a baseline, but they don't by default configure you a highly secure environment. And then lastly, they don't want to make things too complex to work from your business and so that IT can't operate. And really moving on to our third reason, and I'll go into that, it's really IT overload. You can see from these past slides, the licensing, the configuration. It's honestly worse, it's so much worse than even we presented so far.

And that's because it's constantly changing and IT oftentimes doesn't have the budget and resources to look into it. Dedicated security teams, 365 experts, they cost money. People didn't put all this work into doing it just to get paid minimum wage per se. And IT budgets they're often designed to keep things running, to keep support requests down, to keep their email flowing. They're not designed for medium and small businesses, oftentimes they're not designed to have world class security because that costs money, that costs licensing, that costs expertise. And then IT departments don't have the time. Microsoft 365 is constantly changing.

We use Purview as an example. It used to be called compliance and security portal and all the settings for security and compliance. Well then they split it up. Now it's security and compliance, two different portals. And they changed the name. Now it's Microsoft Purview. Just a couple of months all those changes happen, where you find all these configurations all changed and IT departments don't have the time to constantly be looking at Microsoft's release pages and documentation to see where did Microsoft put it this time. They change in meaning, they change in availability. And like we talked about locations and names often change. It's not just the fact that this is complicated, it also has to do with IT being overloaded and not having the resources that they need on their own to configure this properly. And with that, I'll hand it back to Dave. He's eager to jump in.

David Sun: I was clicking and I misclicked, I apologize. Looking through all these questions. We got lots of great questions. We'll get to them. So wrap up a little bit here. Things we're talking about, right? There's barriers to doing this Microsoft 365 securely, and as Nehemiah said and that Dave Hale said, and I said in the beginning, this is not about Microsoft 365 being a bad platform again, we love it, we use it and we suggest it to others when asked, right? We do think it's a strong platform, there's a couple of others out there, but it's definitely one of the strong ones. This is not about it being a bad platform, it's about getting clients or organizations to understand that they're not doing security for you. That's not what's happening. I often hear, go to the cloud, it's more secure, go to the cloud, it's more secure. And that's actually not true.

The cloud is only as secure as you make, and Microsoft 365 and everything we just talked about today is case in point. It can be very secure. But just because there doesn't necessarily guarantee that it is, you the organization need to make sure that it's set up properly for your business practices and how

you operate so that you have the right security for you. Microsoft can't do that for you. None of these cloud vendors can do that for you. Again, that's the barrier, is understanding your environment, understanding your platform, understanding your tool and doing the configuration properly for what your organization needs.

And so what we say is the IT admins and executives with these organizations using it, they sort of have to ask themselves a few questions when they're in Office 365. Is your licensing sufficient? Are you getting the right features you need, not just user features of email and tools and Teams and this that and the other, but as Dave Hale was saying, it's security features also. And most users aren't asking about security features, they're thinking about the user features. And so the IT department needs to be thinking about, are we paying for and buying and having the right security features out of our Microsoft 365 environment. Have we performed a review of our 365 configuration with security in mind? Not just that it works, not just that it allows people do what they want to do, but that it's also secure.

And again, that's always the piece that people unfortunately becomes second to the user side of things. Another question is, does your staff have the budget and bandwidth and expertise to keep up with the latest security changes in emerging threats? Not many do. Not many small medium enterprises do. It's very, very difficult. And so what should you do? Well, you should get a Microsoft 365 security review. If you're looking to move or to migrate, you want to get somebody who understands these issues and is going to what we call harden your tenant, secure your area of Office 365 before you migrate, right? Don't wait until you have data in there, right? Do it before. And part of that is not just to keep your data safe from the minute it lands in Microsoft 365, but it's also makes it easier to deploy that security, right?

Again, security is inconvenience, we understand, and it means users have to do things they don't want to do or can't do things that they would like to do. And so we see it so often where you have a default set up Microsoft 365 and then when you try to secure it later. Now you get pushback from the user base. I used to be able to share links to anybody, I can't do that anymore. Complaint, complaint, complaint, grumble. So take care of that stuff from the beginning and so the users don't come in and they don't even know what they're missing at that point. So secure your tenants before you do the migration. You need to look at making sure that's done. Unfortunately a lot of managed service providers, they don't really have the people on staff. They don't really have the time, energy, resources and expertise to really do that from the beginning.

And this is not a knock on managed service providers. Some do. We've seen some good ones, but a lot of them don't, a lot of them are just doing the default and making sure email stays up, making sure documents don't get lost, that's their benchmark that they're trying to meet and they're not thinking beyond that unfortunately. What have we seen? We offer Microsoft 365 security reviews. They're not very expensive. They're probably one of the most best values that we offer at CLA here for our cybersecurity stuff. Don't get me wrong, a lot of stuff we do is good value, but there's a lot of good value for our clients with Microsoft 365, many of them very appreciative of what they find. We've done dozens of them, I think 40 or 50 security reviews this year.

Over 90% of them have at least one critical security flaw, most of them more, right? The vast, vast majority of our security reviews for Microsoft 365 identify critical security issues in people's configuration. And just to be clear, these security reviews we're doing aren't just for small mom and pop shops. We're doing security reviews for credit unions and financial institution, many of them. And even they are coming back with one or more critical security flaws in their setting. And what are we finding?

We're finding the strangest, we're either finding organizations that aren't doing things or we're finding organizations who are trying, they're trying to do it, but they didn't quite do it right and they didn't understand it.

And so we find organizations, for example, who have these complicated conditional access policies, and because it's so over complicated and they didn't do it right, at the end of the day it just let everything through, right? It's sort of like double negative that they end up allowing things through. We see that. We see policy errors that allow people to bypass MFA, bypass spam folders. Again, people are trying to do it right, but it's new stuff and because it's new, their IT organization, the IT shop is having problems getting it done right. And that's where things are. That's what we're seeing out there, is people either, A, don't know to use it or a lot of times people know to use it and they're trying to use it, but because it's new, they're not quite doing it right because there's a learning curve and they haven't gotten there yet.

We see a lot of that. And that's what comes out in these security reviews that we do. And again, clients, the IT department when they come back and it's very eye opening for IT and others when we give them our findings. So with that, let's go to Q&A. Let me see what we have here in the queue already. And then if you have others, please free to ask. We'll try to get these things answered. We have about 10, 12 minutes. How about one here, maybe I'll throw it over to Nehemiah. What basic security settings do we recommend or can we recommend? Right? It's really how I would ask that because I have my feelings on that. Nehemiah, what do you think? Nehemiah we might be on mute. We might have caught you this time.

Nehemiah Jones: There we go. There's a laundry list of configurations that we can list that we'd recommend. I would say some basic ones are lockdown your conditional access policies and secure service accounts and locations. I would say that. As well as the ones we already mentioned with SharePoint and share settings. I would say conditional access policy is doing a good job, making sure everyone has to authenticate with MFA. And then taking care of even some of the things in this slide with share settings are pretty big.

David Sun: I would say, and the things that Nehemiah hit on are the big ones, but remember we said at the very beginning of slide, there's over 120 different security settings. When I get questions like that, I don't like to answer it, because sure we'll tell you about it, the two or three big ones, but I don't want people walking away, I'll take care of those. Nehemiah told me about doing this five and that means I'm protected. There's 120. So yeah, [inaudible] one, but there's a lot more, right? Let's not get that false sense of security going by that. How about another one, maybe Dave Hale. Can geofencing be tricked by hackers using VPN or something else? For example, if we geofence to the US, does that work?

Dave Hale: Yes, absolutely. Microsoft can do only so much, but it looks at that public IP address and if it's a VPN and to the US and you allow US sign-ins, then yes you can get around the geofencing that way.

David Sun: How about another one, Nehemiah, does enabling third party solutions like Barracuda address some of these concerns regarding retention content filtering? You were talking about that earlier.

Nehemiah Jones: I'll just say this, when we say that you have third party spam filter bypass, IT people are going to tell me my MX record points to my Barracuda, great. That's not sufficient. There are ways that if they guess you're in 365, they can completely bypass it unless you have special things

configured. I don't want to go the whole explanation here, but MX record point to Barracuda is not going to fix your problem for the smart hacker.

David Sun: Great. Dave Hale, how about a couple of things here related to the licensing, what's the best plan for a non-profit? Would a local government be considered a non-profit? Again, we can't take it into all the details, but maybe just touch on that a little bit in terms of if you're a non-profit or if you're a government entity, cost efficient, cost effective, what are some things they should consider with licensing?

Dave Hale: I would definitely take a look at that business premium plan that I mentioned. I think even for nonprofits, you start out with 10 licenses for free that you get, that unlocks you the Azure AD premium for conditional access and all that good stuff. I would definitely look at that for the nonprofit side is the business premium plans.

David Sun: Okay, great. And then another similar one, if you have Microsoft 365 business premium, do you need to do anything else to encrypt emails?

Dave Hale: Yes you do. You have to configure it. There is a sensitivity label, encrypt all, you do have to turn it on and activate the service, but then you can enable the encryption for it.

David Sun: I would add this, right? So you got to enable it, that's one thing. You got to use it, but here's the thing, encrypted emails are designed to protect the data as it gets transmitted from one system to another. It doesn't protect the content of the email when it's on the system. So for example, I might send Nehemiah an encrypted email, yay, that email is protected. But guess what, if a hacker gets into my email account, they can go into my sent items and they'll see the entire contents of the email. So encryption is in transit, it is not at rest necessarily. And so that's not getting you the protection that we're talking about here.

We didn't even talk about compromising data while it's being transmitted. None of the last 53 minutes has been about that. It's all been about data at rest. So let's make it clear that encryption is great, you should use it, but it's not going to solve the kind of problems we're talking about here. Let's see. Let's talk about the Microsoft Secure Score. It's not set up by default. What is that about and how useful is it? Anybody want to take that one on?

Nehemiah Jones: I can go ahead.

David Sun: Sure.

Nehemiah Jones: Microsoft Secure Score is a great tool. It shows you some of the basic stuff that you need to enable to be more secure. It's also somehow of an advertisement for features you should buy of course, but it's not the be all end all of security. If your secure score is high, that's a very good sign. If it's low, you need to fix something like quickly. If you're at average. Average is not good on the secure score just to give you a preview. But there are many additional things that you can and should implement outside of secure score.

David Sun: I would add that secure score's good. It's a good starting point, right? And by everything Nehemiah just said. But I would warn, hopefully you've seen elsewhere, secure score is not covering everything. Of the 120 things we're talking about here and things that we talk about, that we cover in the review, only I would say, I don't know, half, maybe less of them actually are reflected within the

secure score. The majority of the settings we're talking about aren't even touched in the secure score. You could be secure and not have any of over half things we're talking about taken care of and you can have over half things we're talking about taken care of and your secure score may not look great.

It's a benchmark, it's a starting point for you to have a conversation, but it is definitely not a grade that you should rely on. Let's see. Nehemiah, your cascade of [inaudible] seems to have hit a chord. Different questions about guests and sharing. So guests, let's see here. Should you disable anonymous links sharing? Is that a best practice?

Nehemiah Jones: Yes.

David Sun: By definition of guest, is it outside our company? Can you share a document with limited access such as view only? Can you tackle a couple of those concepts?

Nehemiah Jones: Sure. A lot of the answers to can you do things a certain way, is yes. There's almost any configuration you can think of, of guest access or view only, or they can't share items. There are settings that you can configure to do that, right? You just have to know what your expectations are, what do you need? And Microsoft is going to provide pretty much in all cases what you need, whether it be sharing to only these specific individuals, only allowing people to share view access, even going as far as to say only an IT admin can add a guest user. So you can do all those things. And as far as anonymous links goes, that is definitely best practice to disable. And if you have, to have, to have to, then you can set a timeout. Let's say it's only available for 30 days or a week or whatever works for you guys.

David Sun: Great. Wow. Lots of questions. We got a bunch of them. I don't know if we're going to cover them all here. Wow. Here's one. Our highly collaborative organization migrated from Google Workspace to Microsoft 365 years ago. A lot of our users continue to complain about relative difficulty sharing files in SharePoint versus dual drive. Do I have a canned response or do we have a canned response that we can explain while may cause short term inconvenience, more restrictive settings are necessary to mitigate risk? I'll start with this and I'll start with this because of investigations I do. We do a lot of investigations on the part of employees. Okay? We have a lot of companies who are using Google Workspace and I will tell you it can be a nightmare.

Because Google is so good at sharing, it makes it almost difficult for an organization to understand what shares have gone out and who's sharing what. And so this person here asking the question, I hear your pain, but I would say this, very few of my clients who have been subjected to an insider threat where departing employees have stolen documents remain on Google Workspace afterwards. I'll just answer it that way. Let's see. Wow. Let's see. Look, there's a lot of questions about getting an Office 365 security review. If that's something that you guys are interested in and you want to know about pricing or possibilities, more than happy, please post up, we'll follow up with you separately on that.

The goal here isn't necessarily to focus on that, the goal here of the webinar here really is to get people to understand that 365 can be an issue and you need to get your IT people or somebody to help your IT people out to really lock it down properly, right? The goal is to get you to understand what the risk is because most people don't. They just think it's safe. And once you understand what the risk is to do something about it, which means talk to your IT and if it doesn't understand what the issues are, come talk to us and we'll talk to your IT. That's fine too, right? That's easy peasy. We talk to IT people all the time and we try to get them to understand what the nature of the issue is.

Let's see. We got a minute left, not even that. I guess with that maybe we'll wrap it up. Again, if there's any ongoing questions or follow up questions we didn't get to answer, I apologize. There's our contact information there. Please feel free to reach out to Dave Hale, Nehemiah Jones, or myself, we'd more than happy to have a longer discussion with you or with your IT person if that's what you need. We want you all to stay safe, keep your data secure and let us know how we can help you with that, right? I think with that we will wrap things up. And again, thank you all for your time and attention. We really appreciate it.