Help Me With HIPAA Podcast Education Documentation Form

On _____, _____ listened to the following podcast episode for additional HIPAA Compliance education.

This May Be Bad For MSPs - Ep 585

November 6, 2026



Imagine enjoying a nice evening at a whiskey festival when a message pops up about a major cyberattack. Talk about a buzzkill! That's how the news of the ConnectWise supply chain attack entered the picture, and it raises some serious questions for MSPs and healthcare organizations alike. What happens when a trusted vendor's credentials are compromised? What if your backups suddenly stop working? And how do you respond when nobody can tell you exactly what's happened or when things will be back to normal? This week, we're digging into those questions and discussing why understanding your vendors, your technology, and the risks they bring is so important.

In this episode:

This May Be Bad For MSPs - Ep 585

Today's Episode is brought to you by:

Kardon

and

HIPAA for MSPs with Security First IT

Subscribe on Apple Podcast, Share us on Social Media, Rate us wherever you find the opportunity.

Great idea! Share Help Me With HIPAA with one person this week!

Learn about offerings from the Kardon Club and HIPAA for MSPs!

Thanks to our donors. We appreciate your support!
If you would like to donate to the cause you can do that at HelpMeWithHIPAA.com

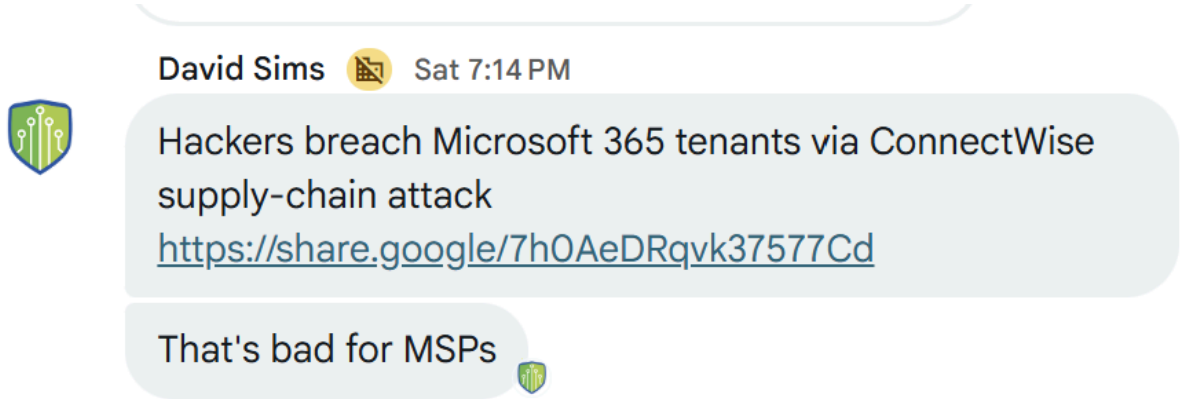
Episode Roadmap

[00:00] Why Tabletop Exercises Show What You Can't Know in Security
[00:33] A Whiskey Festival Interrupted by an MSP Cyber Incident Alert
[02:22] ConnectWise Supply Chain Attack Hits Microsoft 365 Tenants
[05:43] MSP Vendor Consolidation—Pros, Cons, and Hidden Risk
[07:17] Timeline: ConnectWise Detects, Responds, and Goes Public
[08:31] Microsoft 365 Tenants: The "Office Park" Analogy for Healthcare Teams
[12:22] How Attackers Piggybacked on Vendor Credentials—And Why It Matters
[13:26] Email, Files, and PHI: What's Really at Risk in These Attacks?
[17:23] Backup Outages: Planning for When Your Usual Tools Go Down
[20:51] Why Every Healthcare Practice Needs a Real Software Inventory
[24:29] Guidance for MSPs and Clients: Communicating and Handling Third-Party Breaches
[34:26] Every Vendor Brings Risk—How to Talk About It with Clients

This May Be Bad For MSPs

Donna was enjoying a Whiskey Festival on Saturday night. She got a message from David that made her stop and have someone hold her tasting glass. A quick look at the headline generated a verbal response that wouldn't make it through our internal version of the FCC (AKA Karla).

The headline? Hackers had accessed Microsoft 365 tenants through a ConnectWise supply-chain attack. David's assessment was simple: "That's bad for MSPs."



Hackers breach Microsoft 365 tenants via ConnectWise supply-chain attack

ConnectWise (SkyKick) Vendor Credentials Abused in M365 Attacks

Hackers Use Compromised ConnectWise Credential to Sign In to 173 Microsoft 365 Tenants

Trust Center | Advisories | ConnectWise

Upon discovery on October 14, 2026, ConnectWise initiated internal and external incident investigation and response actions.

October 16, 2026 first post about it on the public advisory board.

The activity occurred October 15. Huntress documented unauthorized authentication from an unusual external IP address.

What happened in terms we hope everyone can understand.

It is always fun to explain these things.

What is a Microsoft 365 tenant?

Think of it this way: all these vendors that have things in the cloud have giant office parks that they control. When you buy products from them you become one of their tenants in their giant office park. Sometimes it's a whole building, sometimes it's just the floor or a single office. When you sign up for MS365 you become a tenant of that section of the giant MS office park.

So you can understand, when they say there are 173 tenants, that it's hard to judge just how big this is. We also know that often those first numbers that come out end up becoming bigger. It is very early in the saga so we won't know for some time.

What does it mean that "vendor credentials" were abused in the attack?

This wasn't a stolen employee password. Attackers used compromised application credentials associated with ConnectWise Cloud Backup, formerly SkyKick, to authenticate into customer Microsoft 365 environments. The applications already had extensive permissions.

Now take our giant office park. There are many companies that run cleaning services throughout the giant office park and they get access to the tenants who hire them. They may not have access to everything in that tenant's office. They can go in and do the work they're hired to do, but maybe not every part of the office. One of the cleaning services' clients may have multiple offices across the giant office park. Imagine if someone tags along with the cleaning service and the cleaning service may not even notice they're right there with them. Once they see them go in, they can then go back on their own without the help of the cleaning service. Once they're in there, they can look around and potentially get into areas that the cleaning service didn't even have authority to get into because they've used a variety of tricks to break into those areas.

The attack involved more than one ConnectWise application. Huntress identified abuse involving Cloud Management applications for Exchange Online, Teams, and SharePoint.

Okay so what do we know about how bad it is?

In two tenants, the attackers escalated privileges. Huntress documented a ConnectWise application obtaining Global Administrator privileges and adding credentials to two other applications. That's especially concerning because disabling the original application doesn't necessarily remove access established afterward.

(Huntress has now confirmed attackers established additional access in two Microsoft 365 tenants by granting administrator privileges and adding credentials to other applications. In their most recent update.)

What makes this a problem is you can't just disconnect the way they got in. You have to evaluate and look for any suspicious activity if you know they got in. Or think they might have.

Seven ConnectWise application identities were disabled on October 17, including Cloud Backup and Cloud Management connections. ConnectWise warns that disabling them doesn't undo changes attackers may already have made.

A second, targeted wave of attempts aimed at specific sectors. Huntress identified unsuccessful attempts against 16 additional tenants in sensitive sectors, including national security and critical minerals. Most didn't use ConnectWise products. This suggests the attackers may have been looking for particular targets, not simply exploiting every available customer.

No observed successful activity since October 17 at 05:00 UTC, according to ConnectWise, within the environments it monitors.

Backup archives reportedly remain secure, but ConnectWise explicitly says that alone does not establish whether live Microsoft 365 customer environments were affected.

So what happens now?

Backup and security services are still down. As of ConnectWise's October 19, 13:45 UTC update, Cloud Backup, SaaS Security, and Cloud Management remain suspended. No scheduled backups, archive access, restores, or affected security monitoring. No restoration ETA.

And now we wait.

One of the toughest parts of dealing with a security incident is accepting that sometimes you just don't have all the answers. You may not know exactly what happened, how far the attackers got, or when everything will be working again. That's why we talk so much about tabletop exercises, incident response planning, and knowing what you're depending on before something goes wrong. Whether you're an MSP or a healthcare organization, you need to understand the risks your vendors bring and have honest conversations about how those risks are being managed. You can't plan for every possible scenario, but you can make sure you're not starting from scratch when the unexpected happens. And remember, just because it's someone else's security incident doesn't mean it won't become your problem!

Remember to follow us and share us on your favorite social media site. Rate us on your podcasting apps, we need your help to keep spreading the word. As always, send in your questions and ideas!

HIPAA is not about compliance,
it's about patient care.™

Special thanks to our sponsors Security First IT and Kardon.