Ransomware and Database Corruption, What's the Difference?

Steve Stedman and Derrick Bovenkamp explain the difference between ransomware and database corruption. We offer SQL server corruption repair and even Emergency repair. Generally we will have you up and running again within **24-48 hours!** Schedule a free 30 consultation and see how we can help.

Transcription:

Steve Stedman 0:05
Let's take a look at how ransomware relates to your SQL Server. Now, if you've ever had ransomware, and I know Derek said, sends chills up your spine, and this is one of those things that sent chills up my spine, the situations where we've been called by people with ransomware, needing help, those are some of the most unlikely to recover scenarios. So a couple of differences here that we'll take a look at between corruption and ransomware. With corruption, it's usually something that we can fix. And or at least recover part of it, if not all of the data. And the goal is usually restoring all the data, but with corruption, parts of the data file may be destroyed. But they're not completely gone. There's something there. That's incorrect, that needs to be fixed.

Derrick Bovenkamp 0:47
Yeah, and I think I'll add on to that, before kind of ransomware is, you know, even if it's not completely recoverable, you can usually get it fixed enough and be able to tell the client what, what what is missing or what might be missing, but it's still Yep, the rest of it still working with ransomware. You know, typically, the entire file is encrypted. A lot of times we've seen even paying the ransom doesn't help. We've been called by clients that pay the ransom. And even after running the unencrypted one, it's still you know, the file is still so corrupt. It's like the raid 50 scenario where there there is no repairing it. Yeah, I'd say this is this is one of the toughest things that Steve and I see. Because, you know, we never wish corruption on anybody but, you know, corruption that we could at least do something about, and help them. And a lot of times with ransomware, there's nothing that we can do to help our customer.

Steve Stedman 1:47
Absolutely. Now, with corruption, we can help with the repair. And although backups are great, because of the backups, you've got a view of what things look like before the corruption head. But oftentimes with corruption, we can do the repair, even if you don't have backups. Now, that's not an excuse to not have backups, because there's no excuse for that. But with ransomware, your backups may be your only option.

Derrick Bovenkamp 2:12
Yeah, and I just can't reiterate that enough is we've we've talked to multiple people who their only option was to pay and they paid and they got other files back. But their large databases were corrupt beyond repair.

Steve Stedman 2:28
Yep. And we've seen this where they were running their SQL backups on the same drive the same like D drive on their SQL Server, the same drive as their data files were on, which is, of course, a really, really bad idea. And you would expect that those would be corrupt when you got hit with ransomware. But even those that were doing backups to a network location that was off of that machine, the ransomware is smart enough to go through and go and encrypt all of those backups. Of course, it can encrypt the SQL Server files while it's running. So what it does is it shuts down the SQL Server and reboots it and then encrypts it as it comes back online. So ransomware Yeah, that's way different than corruption. And really, the only safe way is to have off site backups to recover from that are in some kind of cold storage where you can't they can't be changed by ransomware.