Ep #36: Loss Prevention: Avoiding the Minefields in Dental Practices with Steve White

Full Episode Transcript

With Your Hosts

Dr. David Phelps and Evan Harris

Ep #36: Loss Prevention: Avoiding the Minefields in Dental Practices with Steve White

You are listening to the *Dentist Freedom Blueprint* podcast, with David Phelps and Evan Harris. Navigating you through the uncharted waters of a turbulent economy with straight-forward advice to, transform your practice into a self-sufficient cash machine, compound your net worth assets, and multiply, multiply, multiply your passive cash flow streams.

David: This is Dr. David Phelps of the *Dentist Freedom Blueprint* podcast. Today my cohort, Evan Harris, and I are interviewing Mr. Steve White, who is the Vice President of Sales and Marketing of Liptak Dental, the maker of DDS Rescue. This interview is all about loss prevention, avoiding the minefields in our practice. Those minefields that can cause a potentially huge loss. Listen in as you'll get some really great tips and strategies for preventing this kind of a loss.

Hey, everyone. This is Dr. David Phelps back with you with another one of our podcasts with the *Dentist Freedom Blueprint*. I've got my cohort, Mr. Evan Harris with me. Evan, how are you doing today?

Evan: I'm doing great, David. Thank you for having me on the call. I'm looking forward to our guest that's going to be joining us.

David: Well listen, Evan, you were the one that connected me to this gentleman. I'm going to let you do the formal intro but what I found out after doing a little bit of research and talking to our guest is that there are some minefields out there that we can as professionals, as dentists, we can easily step into without even knowing they're there. We're all about building our wealth, building our practices, creating freedom in our lives. But if we're not careful and we don't take preventative action against some of these areas, they can be fraught with danger.

So without any further ado, let me let you, Evan, introduce our guest today and let's delve into this topic of prevention.

Ep #36: Loss Prevention: Avoiding the Minefields in Dental Practices with Steve White

Evan: I'd be glad to. I really want to stay positive and I love talking about wealth building and practice building but in reality, just recently I had a practice that has suffered a significant loss. To come out from underneath that loss is a lot of work. I really want us to talk about how to get more new patients or how to build someone's wealth through real estate but in reality, there's some things going on now that didn't exist just five years ago.

This guy walks in, gives a presentation, his name is Steve White, he's a Vice President for Liptak Dental and DDS Rescue. That doesn't mean anything to you but the dude has been in dentistry for 39 years. I've been in for 21 so this guy, to me, 39, he knows a thing or two. He comes back from back in the day, the G.V. Black "extension for prevention," all of that kind of stuff when we didn't even have computers at the front desk. Now we got computers everywhere. I mean, most of my doctors have two computers in their room or at least one with two screens.

There's just so much valuable data flying around wirelessly and unfortunately a couple of my practices have been nearly shut down. Not shut down because the compressor went out or vacuum went out, but shut down because their data went down, their computer. We're not talking about just one computer, we're talking about the whole server. The whole network.

When Steve came in to talk to us, he shared some ways, not only to prevent these issues from happening but what if they do happen? How to be able to handle it. How to get back on people and back on your feet and start treating patients. Imagine if there was an electrical storm and it shuts off all the electricity, yeah, the office is down. But imagine being down without any patients to be able to call. People are walking in this office, patients are walking in, and they have no idea who

they are, what time they're supposed to be, what hygienist is supposed to see them, bad scene.

So Steve White, I'm thankful for you to be on the call. Could you please just introduce yourself? Give us a little background about who you are and then we can dive in on how you're able to serve these doctors at even a higher level these days.

Steve: Evan, thank you. And David, thank you for inviting me to be part of this today. As far as an introduction goes, yes, you are correct. I am the head of sales and marketing for Liptak Dental, which four years ago started as a company in Southern California taking care of dental IT. Prior to that I have had as you said, 39 years, and yes, that does put a few years on the calendar, of manufacturing dental equipment and marketing it globally, not just nationally here. And had a very good and very long career in product development and marketing and sales.

It's been a fun road and this last four years has been a very interesting learning curve where we've gotten into IT for dental only. What started this whole journey is that this small IT company called Liptak Dental started running into problems like you were saying, Evan, of offices that just simply didn't have their data backed up. Stepping back, like you said, a few years ago no one really cared about it.

The facts are ten years ago, the average office didn't even have one or two gigabytes worth of data to even be concerned about. If that computer stopped working, it was not an inconvenience except for possibly scheduling. But then again, the schedules were all printed out and hung in each operatory. So there was no breakdown or lack of business continuity if you will. That has changed drastically. Four years ago, the average office had roughly 45 gigabytes worth of data and now it's jumped up to

90 and growing at 20-plus percent a year. It's really exploding. What hasn't gone along with it is the management of that data.

We developed DDS Rescue as a way to bring business continuity that is used in all of the manufacturers that I've dealt with, that you at Patterson Dental use in your corporate office. To make sure that no matter what happens, whether it be an electrical storm like you mentioned, or a server failure, or a crash, or a disaster, that the business keeps going. In our world, that means continuing to see patients and having all functions of the office work, be it digital radiography, billing, receiving, whatever. We developed that because of the lack of good backups.

Now, as you mentioned, some things have come up in the last, actually, two years since September 2013 that have changed the landscape. Business continuity is exactly what we were just talking about. It boils down to the fact of, if your server can't run your office network, we have to be able to step in and do it. No matter what challenges that server. Now as I said when we originally started, it was the server failed. A disaster happened.

But the challenges and the landscape have changed drastically since September of 2013 and that was when the very first ransomware, which is a type of malice software, or malware, if you will, was detected. That happens to be something that was called CryptoLocker. In a very short period of time that ransomed by encrypting and closing up servers and then starting a digital clock on the screen that says that if you the owner of this computer don't pay them X number of hundreds of dollars within 72 hours, is usually the time frame, we're going to lock your server up forever. You'll never get the data out of it.

Evan: Steve, can I ask you a question?

Steve: Sure.

Evan: So what I'm hearing about is years ago is viruses, all about viruses, and they were typically some 15-year-old kid with five Mountain Dews in him with pizza just creating these random algorithms or whatever they were just to mess with people, but there was really no way for them to win for someone else losing.

But what I'm hearing now is there's a method where someone can create somewhat of a virus, something that can take over someone's computer and can be able to actually destroy or misfigure information and they're asking for money in return to not damage their data.

Steve: Absolutely. They're asking for money and say, "If you don't give us money we're going to keep your server locked." If you do give us money, supposedly, and a fair amount of the time, they give you a code or a key if you will, an electronic series of numbers and letters to unlock that encryption. So you've unlocked your server and you can get back your data. So you're absolutely correct.

In fact, the charting that was done the first two full months that CryptoLocker was being tracked in the late 2013 they followed the account where this currency, which happens to be called bitcoin, was going. They found 24 or 26, can't remember which it is but it is one of those two, million dollars US currency value already collected in two months.

Evan: David, do you think we should have one of those guys on the call? How to increase your wealth through ….?

David: Well, that's not quite the strategy that I would espouse but let me ask you, Steve, then who's at risk? Who is at risk for this

ransomware, CryptoLocker? Then obviously tell us what you're able to do to help offset that risk.

Steve: To answer your question, virtually everyone is at risk for this. Anybody that's got a computer and does anything with the internet at all. Everyone is at risk. How we can mitigate those risks is somethings that we've backed into. Like we were talking about yesterday, we hadn't really gotten involved beyond the normal business continuity of failure of servers. We hadn't really run into this until the first Saturday of this year, January, I believe it was 2nd when the other half of the problems that we're now facing raised its head with one of our customers.

That was the fact that we detected the server that they had--because we do monitoring--was not responding. We contacted the doctor and come to find out, her server had been stolen. Now mind you, I need this to be said, this office, which is in Northern California had done everything compliant with HIPAA. Everything. Her server was stolen. We worked very closely and still do with that office helping them trying to recover from that theft.

Theft had not been an issue in our industry until recently. The most recent HIPAA report, which was released in February of 2014 says that of data breaches, 48 percent of them, which was the year of 2013, were from theft. Not loss. Not hacking. Theft.

Now the problems that came from that afterwards is this office having to go through the data breach notification rules for HIPAA has put themselves in such a situation that in the first seven months, from January until August, the expense level had just crested $100,000 for HIPAA consultants, HIPAA attorneys, notification, insurance for ID protection, and a few other steps.

Ep #36: Loss Prevention: Avoiding the Minefields in Dental Practices with Steve White

Evan: 100k? $100,000.

Steve: HIPAA has not been involved in any lawsuit. $100,000 in seven months plus …

Evan: Think of the amount of money that could be invested, right there.

David: Well, sure.

Steve: Plus, the consultant is projecting that this office is going to lose somewhere between 25 and 30 percent of their patients. Now there's a hit that's very serious and it comes from having to do the HIPAA breach notification by the rules. So this kind of pulled us into this where we were just dealing with server failures. What we have done since January is gotten very, very much involved in taking our business continuity solutions and making sure that we learn as much as we can about these two new threats, which is ransomware, which by the way is much more frequent than theft, at least in our customers, and the theft and how to make it such that we're going to mitigate the possibility of it happening.

But as Evan said, once it happens, we've got a protocol on how to get you out of it. That's the important part because we need to not only be able to recover quickly so you continue to see patients but we've got to keep this cost down that could be associated with the ransomware, the loss of time, the loss of data, the HIPAA concerns, the notification of patients. It's a whole new series of threats that like Evan said, two years ago never even existed. We are addressing them now more than server failures. This is a majority of the time spent now, roughly 75 percent of our technician's time is not spent working on servers in offices that have failed. It's ransomware is number one and number two is theft.

Ep #36: Loss Prevention: Avoiding the Minefields in Dental Practices with Steve White

David: Okay, let's talk about the theft part, Steve, because this is something I asked you the other day and I was not even aware as to why somebody would want to steal a server. But you explained it to me and then it made sense so let's go down that path a little bit, describe the ramifications.

Steve: Well in January when we got this notification and started working with this office, I absolutely assumed it was because somebody wanted the patient information because we've heard since HIPAA came into existence that patient information is valuable, significantly more valuable than credit card information. I assumed it was for the health records and I was wrong.

What the target seems to be is because of identity theft and as *60 Minutes* has now shown twice, once in September of 2013 and again in June, I believe it was 28th of this year, 2015. There's a new tax scam out there and all they need are valid date of births and social security numbers. Don't need your name. Don't need anything else. They're valuing this information at $1,000 per list of 100.

Now the average server has patients or records of roughly 5,000 or more, 5,000 to 7,000. On the black market, that's $50,000 to $70,000. In this same segment from *60 Minutes*, twice they were asked, "How easy is it to get?" They're saying it's very easy. They're saying, "Where do you get them?" Twice they mentioned dental offices. Once they also mentioned medical but they mentioned dental twice. If you stop and think about it, if you walk into a dental office today, as Evan you do all day long, how many places do you see the server sitting out in the open totally unprotected?

Evan: All the time. I can walk right by the front desk and it's either going to be underneath the desk right there or they might have

a server closet, probably right by the bathroom. Or I'm walking down the hall and it's going to be right there.

Steve: That's exactly it. As one of our best, we call him a savant, he is one of our genius software engineers, has said, "We don't need this very high level of technical ability to hack, that takes a very large skill set." Right now, like is the case with this customer that we've been watching since the 2nd of January, you don't need a hacker. You need a brick to throw through a front window. You've got two minutes to get in, pull three cords out of the back of a server, and run out and you've got a goldmine.

So what we've learned is in the case of a theft, the one thing we want to make sure our customers do is be protected by the definition of the law, to prevent that from being a breach. If you get your server stolen, it needs to be a nonevent. You need to be able to do two things. Have it be such that it's not a reportable incident by all definitions of the HIPAA rules and you don't miss a patient. So you have business continuity and protection. We've developed that. It's not overly complicated but it needs to be thought through because the data needs to be managed. And in this case, protected.

Evan: Okay, Steve, we've got about 5+ minutes, as much as you can, deliver what you guys do, how you do it, how a doctor can be able to prevent it from happening. But more importantly, if anything like this ever has happened or they think it could happen, what do they do?

Steve: First off, as far as ransomware goes, to deal with the one that we see the most, both Homeland Security and the FBI say do not pay the ransom. Now, if you don't have a backup that's valid, you're not going to have much choice because you've got to get your data somehow. But of all possibilities, don't pay the ransom. A couple of reasons: One, a percentage of the time,

you never get the encryption code back. Two, it still takes days. The average is two days to get the bitcoin so that you can pay them and it's four to six days before you get the code. If you get the code.

When you do get the code, the average is, 30 percent of your files are going to be corrupt because by encrypting them and unencrypting them with a less-than-refined program like they're using, they damage your files. So you may end up with 30 or more percent of your files corrupt anyway.

FBI and Homeland Security says don't pay it. If you do it, what you need to do is get your IT person in there and get that server offline and scrub it clean. Literally take it down to bare metal and then reload all of it with hopefully a good backup. If it happens to be a DDS Rescue customer, we're going to run the business immediately so you don't miss a customer and then when that server is clean, we repopulate the server with 100 percent of the data, all of the IP addresses, and everything, and do it very, very efficiently. So you've eliminated the threat.

We also have protocols that we teach the office on how to mitigate the chance of that actually getting to the server. That's more than we can talk about today but anybody that's interested, we do, sponsored by Patterson, free assessments of the offices and then give full written recommendations on what to do. They can acquire that by their Patterson representative or by contacting us directly at www.DDSRescue.com.

David: So, Steve, you said that your company, DDS Rescue, is actually able to keep the business running, even if there is a ransomware attack.

Steve: Absolutely, just like as if the server crashed.

David: Right.

Steve: There's three or four other things that we've done that we don't necessarily sell the items to take care of it but we take the whole office with this assessment through a process of both physical and technical ways to protect everything and then a disaster plan in case it hits. Same thing with theft. One of the first things is I tell every one of the people that's listening right now. The first thing you ought to do is make it hard for somebody to do a snatch and grab. Get your computers out of the sight of any of your patients and lock them up. And I mean, behind a locked door. Make sure it's well vented and air conditioned but get it locked up. If it's difficult for someone to rob it in under two minutes, they're going to move on to somebody else. Now there's a lot of other things that we talk about that will keep you out of trouble as far as get out of jail free card relative to any HIPAA notifications and that all comes to all of our customers. We provide that to our customers totally free of charge.

David: Okay. In the last minute, I just want you to talk a little bit about what we talked about the other day and that is in terms of the consequences of having a reportable HIPAA breach. Take us down that road because that's a dangerous place to be and explain why.

Steve: The pushback from what we're seeing from the customers that have gone through this, or are going through this actually, is you're looking at this one customer, we keep going back to this one office in Northern California. They're eight months into this now. I do not know what the charges are so far but again, this $100,000 plus that she has already paid in a seven month period is not for any lawsuits from patients. It's not any HIPAA fines. It's all the process. And the process is simple. If you

believe you've had a breach of your patient health information and you have 500 records or greater, you have to one … first off, it doesn't matter how many patients you have, you have to let HHS.gov know. You've got to report it to HIPAA through HHS.gov's website. Two, you have to then notify every single one of your patients in writing and if they have passed away, you have to notify their next of kin that there's a possible breach of their information. It is not mandatory, but every single consultant I have heard and every single attorney has said, "And offer personal protection against their credit."

Evan: Wow.

Steve: Three, if it is more than 500, which every server in every office that I have ever run into would qualify as, you must then do a complete announcement in the form of a press release to all news outlets in your region. That's print, radio, and television. The pushback from this is massive. As is the case that we're watching now and others that we have been watching, the significant inability to recruit new patients because of the negative publicity, and the loss of existing patients, plus the actual expense of going through it, and the time that it takes, could very well be a practice killer. It scares us to the point that we have developed these additional ways to have our customers be secure that, one, it will be hard to rip it off and two, if it does, it is not a HIPAA violation. It is not an occurrence because nothing would leave that office that is not encrypted at a level that the government says is safe and does not constitute a breach.

David: Well, Steve White, that sounds like that's an ounce of prevention that can go a long ways. Technology is wonderful and it allows us to do so much more today in this modern world but it also comes with the unintended consequences that

you've well laid out today. Evan and I surely thank you and our listeners thank you for your time, your expertise. Mr. Steve White with DDSRescue.com. If you have questions or need more information, seems to me you guys are the go-to people for all things in terms of our digital records, how to secure those and safeguard them against these new predators out there in the marketplace today.

Steve: Well, thank you, that's what we're attempting and so far succeeding in doing and I appreciate both David, your time and Evan, for you inviting me to join you two today.

David: So, Evan, if people like the content today and the podcast, what should they go do?

Evan: If you like the content, please, if you're getting from iTunes, let us know and rate us highly. If you don't, stop listening. Use your time wisely. And if you want to be able to have us cover a topic that we haven't yet covered, tell us that as well and if you want us to go deeper on a topic that we've touched on, let us know. We will be happy to do that. We want to create value for all of our practicing professionals out there.

David: All right, thank you gentlemen. Take care, everybody.

Steve: Thank you.

You've been listening to another episode of the *Dentist Freedom Blueprint* podcast with David Phelps and Evan Harris. The place to be to create your freedom lifestyle with more time off, security and peace of mind. Please subscribe, download the podcast, and share it with others who want to create real freedom in their lives and practices.