url: /your-word-doesn't-count

Title: *MSPs Under Attack: The New Wave of Cybersecurity Lawsuits and How to Protect Your Business*

Image: 10_15_msp_security evidence.jpg

Image Tag: security-evidence

Are you familiar with the term "ambulance chaser"? It dates back to 1897, and references attorneys who actively chased victims as a method of gaining clients. For a term that was created long before computers existed, it has evolved into a surprisingly significant part of the tech world recently. What am I talking about? The new breed of ambulance chasers: attorneys who specialize in cybersecurity breaches.

Maybe you're not concerned. Sure, it would be terrible if your business was sued, but if things went sideways, you could always just walk away from it all, right? Wrong! These lawsuits aren't just focusing on businesses anymore. Now they're aiming at the business owners as well. That's right. Even if you close your business, you're still on the hook. That means your personal finances, your professional reputation, and possibly even your family could be feeling the heat.

The bottom line? The game has changed. The risks to managed service providers (MSPs) have never been higher. If you think your basic business insurance will protect you, think again. The new wave of cybersecurity lawsuits is not something you can turn your back on or ignore. The stakes are high, and people are depending on you to make the right decisions.

So, here's the deal. Attorneys representing clients or employees affected by data breaches are pursuing class action lawsuits armed with one thing that courts care about most: **evidence**. I just have one question for you: When this shifting legal landscape hits you, will you be ready?

The Growing Legal Threat to MSPs

Over the last few years, the number of lawsuits related to cybersecurity breaches has skyrocketed. Initially, these cases targeted the companies that experienced breaches, but now, attorneys have expanded their scope. It's no longer just the breached business under the microscope; the IT providers, owners, and even decision-makers are being named in these lawsuits. And you know what that means? Yep. The MSPs managing IT for these businesses need to be ready.

The potential fallout from these cases is enormous. Attorneys are becoming experts at dissecting security programs and identifying every gap in protection. They gather documentation and damages to build ironclad cases that point the finger squarely at the IT provider who was supposed to be safeguarding the system. In the event of a breach, your standard insurance policy likely won't cover the costs of litigation or a court judgment. Worse yet, if your defenses aren't documented and provable, you could be held personally liable as the owner.

Yes, you read that right: *YOUR PERSONAL ASSETS COULD BE AT RISK*.

Evidence, Not Tech, Wins in Court

If you take nothing else from this discussion, take this: courts don't make decisions based on technical know-how. For them, it's all about ***evidence***. Nothing more. Nothing less.

Judges and juries won't understand your firewall configurations, multi-factor authentication, or patch management strategies. What they care about is whether you have the documentation to back up your security claims. Can you **prove** that your cybersecurity program is robust, dynamic, and improving over time? Can you prove you discussed options with your clients and presented them with the full picture?

Close your eyes for a moment. Picture yourself in the courtroom. Picture the judge telling you they don't care that you put a security program in place unless you can prove it with documented evidence such as detailed logs, reports, and third-party validation. How are you going to answer when you're asked under oath to prove what you've done, how you've improved, and how you've adapted to evolving threats?

Attorneys understand the role of evidence. They are already arming themselves with expert witnesses and cybersecurity documentation to attack MSPs in court. If your defense boils down to "we did our best," you've already lost. The burden of proof is on you to show that your cybersecurity measures were not only in place but were effectively protecting the business.

MSP Owners: You Are Personally Liable

Here's where it gets personal: These attorneys aren't just going after a business; they're going after **you**, the decision-makers, the owners. That means if you make decisions about your company's security practices, you could be held personally accountable. MSP owners across the country are starting to realize that their homes, savings, and personal finances are at risk in cybersecurity lawsuits.

Traditional business insurance doesn't cover these types of personal lawsuits. And even if your insurance policy does have some cybersecurity coverage, it likely won't cover everything, leaving you exposed to enormous financial damages.

The Best Offense is a Rock-Solid Defense

So, what can you do? The answer is simple: **proactively collect and maintain the right evidence**. Your best defense against cybersecurity lawsuits is to have **third-party validation** of your security practices. You need to show, with clear documentation, that your security program is working. This means providing evidence that you've been diligent in applying patches, monitoring for threats, conducting penetration tests, and adjusting your systems in response to the latest cybersecurity challenges.

Third-party validation is critical. It not only helps prove that you are taking security seriously, but it also deflects blame when something does go wrong. In court, third-party reports can make the difference between being held liable for a breach or walking away from a case unscathed.

If you're not proactively collecting and validating your security practices with evidence, you're gambling with your business's future and your personal financial well-being.

Are You Ready to Defend Yourself?

As the legal landscape continues to shift, it's painfully clear that it's no longer enough just to "do your best" when it comes to cybersecurity. You need to prove, with documentation and third-party evidence, that you're doing everything possible to protect your clients.

Galactic specializes in working with MSPs to ensure their security practices are documented and validated. Our third-party validation services provide the evidence you need to protect your business and your personal assets from lawsuits. Don't wait until you're the target of a class action suit. Reach out to us today to learn how we can help you build a rock-solid defense that stands up in court.

Your business—and your personal future—depend on it.

Description Tag:
MSPs, beware: Lawyers are now targeting IT providers in cybersecurity breaches. Without the right evidence, your business and personal assets are at risk.