url: /security-evidence-is-key

Title: *Are You Prepared for a Cybersecurity Lawsuit? Why Documentation is the Key to Your Defense*

Image: 10_15_client_security evidence.jpg

Image tag: security-evidence

There's a movie in the 1950's called, "The Beginning of the End" in which giant grasshoppers take over Chicago. There's plenty of ridiculous elements in this movie, but nothing quite beats the scene where the two main characters, a photojournalist from Washington DC and a scientist from the midwest, encounter the creatures for the first time. Despite having a camera in the car, and the female lead being a trained photographer, they don't take a single picture. The result? Grasshoppers are terrorizing Chicago, while the main characters stand in front of the Secretary of Defense in Washington DC looking foolish.

This is a funny example of the problem with not having evidence. But you know what's not funny? You standing in a courtroom with no evidence trying to defend your organization in the aftermath of a cybersecurity breach.

Lacking evidence when you need it could be disastrous for your company when it comes to cybersecurity. While this may sound overly dramatic, especially if you have worked hard on your cybersecurity, the fact of the matter is that. A growing number of companies are being targeted by aggressive attorneys representing employees, clients, or even entire class-action lawsuits following data breaches.

So, here's the million-dollar question: *Are you prepared to defend your business if it becomes a target?*

Most companies believe they're safe because they've invested in cybersecurity tools: firewalls, antivirus, multi-factor authentication, and so on. But in a courtroom, it's not about the tools you have. It's about the **evidence** you can present to prove that your security measures are effective. Without proper documentation, your business is vulnerable to costly lawsuits that could put both your company's finances and your personal assets at risk.

The Growing Legal Risk of Cybersecurity Failures

Lawsuits related to data breaches are on the rise, and attorneys are becoming increasingly skilled at turning these breaches into major payouts. While it used to be rare for lawsuits to

follow a cyber incident, it's now becoming the norm. And the consequences of losing such a lawsuit can be devastating, especially if you don't have the documentation to prove you were doing everything in your power to prevent the breach.

When your company experiences a cybersecurity incident, it's not enough to say, "We tried our best." Courts don't make decisions based on whether or not your IT department had the right intentions. They make decisions based on **evidence**. And without that evidence, your company could be held liable for millions of dollars' worth of damages.

Even worse, many decision-makers are finding out too late that **they** can be personally named in lawsuits. That means your home, your savings, and your personal financial future could be at stake.

What Evidence Do You Need?

Bottom line: no matter how good your cybersecurity tools are, if you're not documenting your security efforts, you are putting your business at serious risk.

Documentation shows that you have a **comprehensive, active, and evolving security plan** in place. It's not just about having the right technology—it's about being able to prove that your cybersecurity program is functioning, improving, and responding to new threats over time.

This documentation includes things like:

- **Security policies and procedures:** Are your security protocols up to date? Can you show how they have evolved in response to new risks?
- **Audit logs:** Do you have records of who accessed sensitive systems and when? These logs can be critical in proving that you had control over your network.
- **Patching records:** Can you prove that you've been diligent in applying updates and patches? Out-of-date software is often a key point of failure in cyberattacks.
- **Risk assessments:** Have you conducted regular risk assessments? Can you show that you're aware of the vulnerabilities in your system and that you've taken steps to address them?
- **Employee training records:** Are your employees trained in security best practices? Training records can demonstrate that your team is prepared to deal with cyber threats.

The list goes on, but the point is clear: **if you're not collecting and maintaining this evidence, you're vulnerable.** And when attorneys come knocking, they're going to be looking for every gap in your defense.

Your Insurance Won't Save You

Many decision-makers believe that their business insurance will cover the costs of a cybersecurity lawsuit. Unfortunately, that's often not the case. While some policies offer limited coverage for cyber incidents, many don't cover the full costs of litigation, settlements, or judgments.

Even if your insurance policy includes some coverage for cybersecurity breaches, it likely won't protect you from being named personally in a lawsuit. This is where things get especially dangerous for business owners, CEOs, and other key decision-makers—your personal assets could be on the line. Without the right evidence to defend yourself, you could end up losing not just your business, but your financial future as well.

The Time to Start Is Now

So, how do you protect yourself? The answer is simple: **you need to start documenting your security efforts now**. If you wait until after a breach happens, it will be too late. The time to act is before you ever find yourself in a courtroom.

Building a strong defense starts with creating a **documented cybersecurity plan**. This plan should be comprehensive and include everything from risk assessments and patching schedules to employee training and incident response procedures. But most importantly, it needs to be updated regularly and **validated** by third parties.

Third-party validation is critical because it shows that your security program isn't just words on paper—it's been reviewed, tested, and verified by experts. In court, third-party evidence carries significant weight and can help deflect blame away from your company if something goes wrong.

Can You Prove Your Security Plan Works?

At the end of the day, it all comes down to one simple question: **Can you prove your security plan works?** If the answer is no, you are leaving your business and your personal finances exposed to enormous risk.

Don't wait until you're faced with a lawsuit to find out whether your cybersecurity plan holds up. If you don't have the documentation to prove that your security efforts are effective, you need to get started now.

We specialize in helping businesses like yours build rock-solid cybersecurity defenses. We offer third-party validation services to ensure that your security program isn't just good on paper—it's provable in court. Reach out to us today to learn how we can help you get started documenting and protecting your security plan, so that when the time comes, you'll have the evidence you need to defend your business and your personal assets.

Don't leave your future to chance. Start documenting your security efforts today.

Description Tag:
Think you're safe from cybersecurity lawsuits? Without documented proof of your security efforts, your business—and you—are at risk.