Data Security Risks of Third-Party Vendors

Evan Benet December 03, 2020

Cyber and Data Security

The threat landscape for data security is incredibly vast. Today, law firms have the responsibility and duty of technological competence to ensure that their client's information is safeguarded and monitored.

The sad reality is that law firms are often the center of data attacks because of the type of sensitive information that is being dealt with on a daily basis. Often times, attorneys assume that their email or personal information is safe. This is a mistake.

Maybe unbeknownst to you, your personal information includes clues into larger portals of information that can then be categorized and cataloged for hackers to use to gain access to other sensitive information.

Crime today has been commercialized, and organized crime groups use tools to professionally infiltrate your information. The hacking industry now runs much deeper than someone sitting in their basement chugging a Mountain Dew, it has evolved into an illegal business that has cost firms and businesses billions of dollars.

Because of this, clients are no longer just paying for legal services, they are also paying to ensure that their data is protected. Today, class-action lawsuits can be brought against a firm for failure to safeguard and protect their client's information.

An attorney may be required to take special security precautions to protect against unauthorized disclosure of information or when the nature of the information requires a higher degree of security. So, for example, does everyone at your firm have access to the same information? Is it classified and compartmentalized across the firm? Is the data protected according to its sensitivity?

All of these things should lead you to question, are the measures you're taking and putting in place strong enough to protect your client's sensitive information?

At the end of the day, it's about organizing your information in ways that keep it safe and accessible to those who need it. Do you keep all your client files on one hard drive? Do different clients warrant a different type of security to access their files, are they cleaned up regularly?

Model Information and Security Controls

The Association of Corporate Counsel (ACC) published model information and security controls that have been adopted almost nationwide as the defacto standard for attorneys to follow. Whether you have an IT team or not, it is your duty and responsibility to understand these measures and be able to act on them.

Let's go through some of these together:

1. Understand your information

In order to protect your firm's and your client's information, you must understand what information you have. You must then classify and organize it, and then thoroughly document what you are going to do to protect it.

2. Review the rights and responsibilities

You're either doing a good job and following best practices, or you're not. You need to know what procedures you have or will have in place to secure what needs to be protected.

3. Physical security

Does your office and your third party vendor's space utilize badges and door codes? If not, this is the easiest thing to quickly implement. You can also go one step further and store data in different access-based locations and create logical controls so people are only accessing the information they are authorized to.

4. Information disposal

What you do when you're done with the sensitive information should be reviewed and documented with your clients as well. Are you giving their information back? Are you destroying it? Are you doing both? That needs to be outlined and made clear.

5. Monitor

Make sure your people and your vendors are doing what they're supposed to be doing. Conduct vulnerability assessments, make sure your devices are encrypted, and know if something is open or publicly accessible. Encryption is a very basic security measure that your firm needs to be aware of and implementing (if you're not already). Your information should be encrypted both at rest and in transit. For example, if you have an encrypted computer that gets stolen, you don't have to report that because the thief cannot do anything with the information on the device. Yes, you'll be out an expensive piece of equipment, but your data will be secure. That is encryption at rest. Encryption in transit is the protected information that is being sent or received between devices like through email or text.

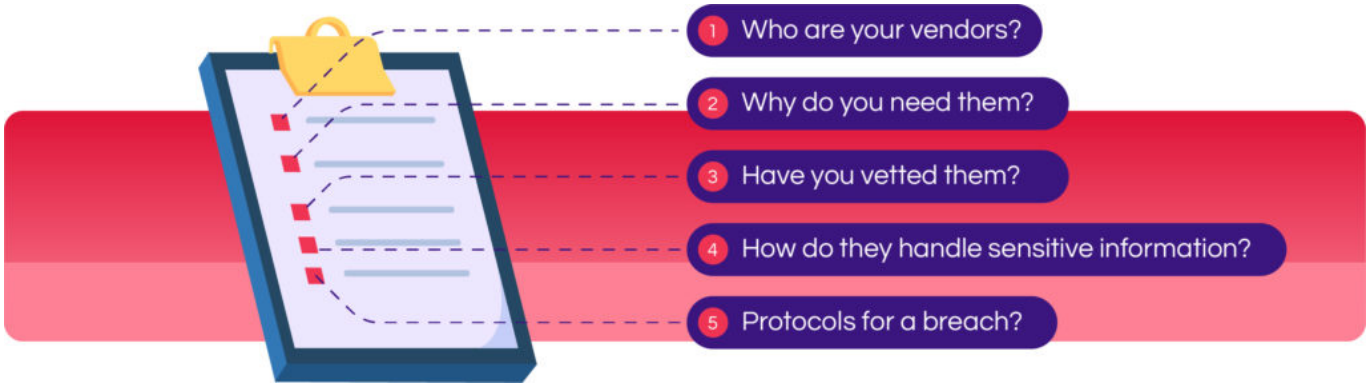
The most dangerous people at your firm are the ones who lead your IT team, but they are also the most helpful. This type of trust is a commodity. There must be controls in place to ensure that the work they have done is accurate and secure. If you do not have an IT team, you need to do your due diligence with your cloud provider or your third-party vendor and ensure that they are up to date with the latest security measures and you have records that they are constantly monitoring your information.

6. Insurance

You don't know what you don't know. Buy cyber insurance. Only 34% of firms have cyber liability insurance. Take the opportunity to limit your exposure because the cost of a breach will end up being significantly more than the cost to prevent it.

Now that you have all this information in place what do you do? You prove it. Take the time to get an industry certification or a privacy shield and be proactive to show your clients that their highly sensitive information is in good hands.

Third-Party Vendor Cloud, Compliance, and Risk Management



Third-party vendors constitute a lot of risk. Did you know that 60% of breaches are linked to third-parties? Even today, many firms do not adequately assess these relationships because they feel that their staff is well trained and will assume their vendors are too.

Let's look at some numbers here:

32% of firms do not evaluate third-party vendor security.

60% of attacks come through third-party vendors.

And only 34% of firms have cybersecurity insurance.

So when someone asks? Why do we care? This is why. These figures are staggering. Even though you may have a buttoned-up security system, can you trust the third parties?

If you're working with third-party vendors, you need to follow some basic steps to ensure that the work they are doing is not only correct but protected as well. Ask yourself:

- Who are you working with?
- Why do you need to work with them?
- Have you vetted them?
- Have you asked how they handle sensitive information?
- What are their protocols for a breach? Have you considered the time frame you will require the vendor to report a given breach? What steps must they take, and who they must contact?

As we discussed earlier because third parties are very susceptible to cyberattacks, clients are asking for assurance from their law firms and as a result, many of these firms are seeing an increase in information security and data governance audits coming from their clients. It is becoming more common practice to audit your third parties, both from the client and firm side because the risks of cyber attacks are so high. At the bare minimum, if you're using a third-party vendor, make sure they are doing at least as good of a job as you are in implementing security controls. Do not assume anything because it is not if you will experience a potential breach, it is when.

What Do I Ask My Third-Party Vendor?

You don't have to be an IT professional to ensure that your firm and your client's information are safe! If you're using a third-party vendor to store your data, consider asking them these three questions…

1. How are you protecting my information?

This is an open-ended question for which the vendor should immediately answer by showing you their security policy documentation, standards documentation, and instant response plan. If they respond with something along the lines of that information being proprietary, you should raise concern. The best practice in security is always transparency.

Additionally, when you ask your vendor any questions regarding your data, pay attention to how they answer it, and take note of the amount of detail they give in their response. They should be able to tell you what they are going to do with the data, how long they're going to keep it, and how the data is classified.

2. What are you doing with my information?

What infrastructure is your third-party vendor using? Where are they physically located? What class systems are their server hardware and firewalls? Using a third-party vendor is a lot of work because you need to do your homework and make sure that your information is secure. For example, look at their data flow diagrams, this will tell you all the buckets where your encrypted data sit at rest and all the paths they take between those buckets when they're encrypted in transit. It is important to ask how they encrypt your information and the humans that are physically accessing that data at each point.

3. Business Continuity Plan

This is your backup plan! Some firms use Amazon Web Services (AWS) as a hosting vendor. Just last week, their system went down. Not for a few seconds or minutes, but for hours. The reason for this outage was undisclosed (scary!). Because of this, you need to know does your third-party vendor have an off-site disaster recovery location to allow for a quick transition? Ask to see what their uptime has looked like over the course of several years and if they have had a lot of impactful outages. Your job depends on being able to access your stored documentation and files. If you don't have access to what you need, you can't do your job.

Key Takeaways

Using third-party vendors may pose many avoidable risks. It is best practice to consolidate your tech stack and make sure you know exactly where all your data is stored. At all times.

When it comes to IT and your security, you need a strategy. You cannot hope things go your way, or hope a backup can be produced. Your clients expect nothing but excellence from you, you should expect the same from your vendors.

And if you remember anything from this blog, remember this- If you didn't document it, it doesn't exist and if you didn't test it, it doesn't work.

If you're still curious to learn more, check out our blog: Data Security for Law Firms: Everything You Need to Know