Law Firms Cringe, But Bow to the Need for Zero Trust Architecture

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Zero Trust Architecture simplified

Lawyers have a "deer in the headlights" look whenever we talk about Zero Trust Architecture (ZTA) - and we do understand that look. ZTA is complicated and often causes your eyes to glaze over about two minutes after we bring ZTA into the conversation.

Let's keep it as simple as a complicated subject can be.

Zero Trust Architecture (ZTA) is not a product you can buy in a store or online. It is a security model presented in 2003 by the Jericho Forum, although the term "zero trust" dates back to 1994. The zero trust model surfaced in 2010 but would take almost a decade to become prevalent. Our old models assumed that users and devices within a network could be trusted and given access to resources based on their location or other factors.

ZTA is different. It assumes that all users, devices, applications, etc. are potentially compromised and must be validated before they are granted any access to a network. And periodically, they must be re-valuated.

In essence, ZTA creates a security perimeter around each user, device or application – rather than a perimeter around the entire network. Now you have more granular control over access to resources. The perimeter security model doesn't work as more and more firms move to a hybrid work environment or even complete remote access. ZTA drills down to smaller objects and is well suited for a mobile workforce. What does that mean to your firm? You stand a MUCH greater chance of defending against cyberattacks – and of limiting the damage that an attack may cause. Now that's a goal worthy of effort and money.

What steps do you need to take to implement ZTA?

There are a lot of steps to take, but here are the basics.

- Identify all users, devices and applications that need to have access to resources on your network.
- Verify the identity of each user, device and application prior to granting access. How do you do this? You use multi-factor authentication, device profiling and a long list of other methods.
- Limit access to the resources that are necessary to perform particular functions, using access controls and role-based access.
- Monitor (24X7) activity on the network so that you can be alerted to any suspicious activity. Use advanced analytics and machine learning.

- Encrypt all data at rest and in transit to ensure there is no unauthorized access.

Why is it so important that law firms implement ZTA?

As all lawyers should know, their firms are one-stop shopping for cybercriminals. Break into a normal company and you (mostly) get data about that company. Break into a law firm and you've got data about a lot of people, companies, organizations and often, governmental entities.

Much of the data may be deeply confidential (medical data, financial data and intellectual property, etc.) and law firms have an ethical duty to protect that data. In the event of a data breach, there could be major legal and reputational consequences. With perimeter security being a broken model, there is really no choice but to move to ZTA. To be ethically competent with the technology we use, there is no other pathway.

At this point in time, law firms are connecting to their network and cloud services from many different locations – and the people connecting may be clients, employees and third-party vendors. All of this necessarily increases the risk of unauthorized access.

ZTA can help truly secure law firm data, hardening the firm's overall security defenses. It helps firms meet compliance and ethical requirements – and it sure as heck demonstrates to clients that the firm takes the protection of client data very seriously!

Ethics and ZTA

When we lecture, we are often asked if ethical rules **require** that law firms adopt ZTA. Explicitly? No. But they do require that lawyers take "reasonable" measures to safeguard client data. Both the duties of competence and confidentiality require that. Very soon, within the next couple of years, no one is going to question that ZTA is "reasonable" and must be implemented. Better to start down that path now and be prepared.

Failure to move to ZTA may well, one day in the near future, be construed as failing to take reasonable measures to protect client data from unauthorized access or disclosure – and that might lead to disciplinary action or legal liability. And, as we note below, clients and cyberinsurance companies may require the implementation of ZTA.

OK, you're sold. So how much will it cost to implement ZTA?

Boy oh boy, do we wish there was an easy answer to that question. Obviously, a lot will have to do with the size of the law firm. Some firms need a greater level of security because of the data they hold. Some firms have a very complicated IT infrastructure, others (especially the smaller law firms) do not.

You will have hardware and software costs for sure, including such things as firewalls, intrusion detection systems and access control solutions.

Configuration and integration costs will be incurred as you integrate ZTA into your existing IT infrastructure. The bigger your firm, the more that will cost.

You'll need to budget for training. Employees need to understand ZTA and be comfortable using the tools that come with it. They need to get used to access controls, multi-factor authentication and other security practices. Though the training is essential, it is unlikely to be a big cost for a smaller firm.

Maintenance and monitoring costs are also a factor. There will be ongoing updates, maintenance and monitoring on a 7X24X365 basis, with alerts likely going to a human-staffed Security Operations Center (SOC). Not to worry. There are affordable outsourced solutions available to implement a lot of the Zero Trust Architecture, even for small firms.

Overall, a small firm is looking at thousands of dollars, but likely not tens of thousands of dollars. The price tag goes up the bigger you are. As you groan about the price tag, bear in mind the much larger costs associated with a data breach. That may make your ZTA budget seem a little more palatable.

Still not persuaded? Need to understand why perimeter security won't protect you?

We're not surprised that we have to go over this ground again and again with clients. Perimeter security worked and worked well for a very long time. But with the prevalence of cloud computing, mobile devices and remote working, its effectiveness has eroded. Without a traditional perimeter, it becomes increasingly difficult to control access to data. It becomes easier for a cyberattack to succeed – and not by a little but by a lot.

Cybercriminals spend a LOT of time using techniques which will overcome a perimeter defense. These techniques include phishing (the big kahuna), social engineering and malware designed to defeat perimeter security. There are a lot of techniques – it takes us an hour to go through them all when we do a one hour lecture so forgive us for simply touching on the highlights.

Remember that it takes just **ONE** compromised VPN connection to pierce your perimeter security wall. And once inside the perimeter, the cybercriminals can move laterally through your network and do a world of damage, including deletion of backups and massive exfiltration of confidential data. ZTA is the inevitable upgrade you need.

Are cyberinsurance companies beginning to insist on ZTA?

Yup, they sure are. They may not explicitly demand it (yet) or even use ZTA terminology, but they are on the way to doing so. They certainly encourage all moves toward ZTA and premiums will be less the more you take steps to implement ZTA.

Today, insurers want to see multi-factor authentication. No ifs, ands, or buts about that. They also want clients in the cloud, where they are safer. They often require that you have technology which monitors for a data breach. They want all laptops used for work to be owned by and protected by the law firm – no access by personal devices. They want encryption everywhere too.

The list goes on and on – but you get the idea. Every new requirement is moving the insured closer to true ZTA. Expect that trend to continue. And if you don't do what they want, they may deny coverage

altogether or limit the amount of coverage. Every time we sit down with a client to go over a cyberinsurance application, there is much gnashing of teeth by the client.

Are clients beginning to insist on ZTA?

Absolutely. The larger the client, the more they are likely to require cybersecurity assurances from their law firm(s). Even less sophisticated clients are beginning to ask questions and demand cybersecurity assurances from their law firm.

In a world where clients hear about data breaches daily, it is no wonder that they are not only looking at their own internal security but that of their law firms. Law firms, especially the smaller firms, are not noted for first class security. In March 2023, a single cybersecurity company reported that it had dealt with data breaches at six law firms (not identified by name) in just the first two months of 2023. Imagine how many law firm breaches were dealt with by **all** cybersecurity firms in the same time period.

Clients are currently dictating that certain security measures be followed – and larger clients may be requiring that ZTA be implemented. In some industries – healthcare and finance are good examples – there are regulatory requirements that the client AND the law firm may be bound by.

One more thought re: ZTA for law firms: Firms which implement ZTA are becoming more attractive to clients. That's something to think about as part of your marketing and client retention strategy.

If your head hurts from reading this article, a good resource is Microsoft's Zero Trust Guidance Center which may be found at https://learn.microsoft.com/en-us/security/zero-trust/

Final words:

We'll note one last time that "perimeter security" is dead. That's what makes ZTA so urgently needed. So, if you choose to turn a blind eye to ZTA, remember the words of Benjamin Franklin: "By failing to prepare, you are preparing to fail."

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com.*