Cybersecurity basics are important for sophisticated lawyers and firms too (and everyone else)

By John Bandler, Esq., Bandler Law Firm PLLC

APRIL 16, 2026

Cybersecurity basics are not just for newbies, luddites and simpletons. They are for everyone, including experienced and sophisticated individuals, attorneys, law firms and other organizations.

Alas, the basics are frequently ignored and rarely get the attention they deserve.

Let's face it, we are in an attention economy, and basics seem boring to some at first.

But suppose we ignore the pull of cybersecurity marketing hype which try to draw us to products and services which purport to solve cybersecurity problems without the need to expend time and effort. We can also ignore the distraction of flashier topics of the day.

For the next thousand words we can focus on the facts and logic of these basics because we realize it is hard to excel on anything when skipping the basics, hard to address complexities when basics are neglected, and many failures and disasters happen because the basics never got done.

What are the basics?

We've covered some parts of the basics in prior columns and recap here (notably "Build your cybersecurity program in your firm or organization," Reuters Legal News, Dec. 15, 2025, https://bit.ly/4kBDED4).

Cybersecurity organization basics start with management, and that means organizations need to build and maintain a cybersecurity program and properly manage their information systems to help the firm do its job better and prevent disasters. Management includes putting a person (or group of people) in charge, establishing organization rules (including a written policy), due diligence on cybersecurity and technology issues, and then making sound, defensible decisions.

With a management process in place, certain things need to be done, and my Four Pillars of Cybersecurity offer a way to step through these basics. It starts with (1) build *knowledge* and awareness (to facilitate good decision making), (2) secure computer *devices*, (3) secure *data* and online accounts, (4) secure *networks* and use of the internet, and then repeat.

Cybersecurity organization basics start with management, and that means organizations need to build and maintain a cybersecurity program and properly manage their information systems to help the firm do its job better and prevent disasters.

As we work to secure devices, data, and networks, we need to first learn what we have. We can think of it as an *exciting journey of discovery about our information systems;* a scavenger hunt game where we learn about all the digital assets held by the firm.

In simpler language, this is just more of the basics, summarized as: *Inventory your information assets.*

When firms don't do these basics, they forget about the essentials. They forget about their domain registration, until it is hacked or expired and then their website and email stop working, which is a disaster. They forget about — until something bad happens — the hardware devices, online accounts, and the copious data which they have stored and stashed here, there, and everywhere.

Why don't the basics get done?

Cybersecurity, including the basics, takes time and effort but generates no revenue for the organization. This presents various dilemmas according to organization size.

Larger organizations employ information security and technology professionals who have no requirement to generate revenue, and their workday can focus on managing and protecting information assets. The organization made a conscious budgeting decision to devote significant resources to this area, and it becomes a person's full-time job to ensure the basics get done.

Cybersecurity, including the basics, takes time and effort but generates no revenue for the organization. This presents various dilemmas according to organization size.

Organizations and firms of smaller size could not possibly hire a dedicated employee for information security but still have commensurate needs and duties to secure information systems and manage them effectively.

That means cybersecurity responsibilities need to be added upon an employee's existing duties, even though that person already has a full work week, potentially with revenue generating responsibilities and other management duties. Some firms neglect to assign anyone these cybersecurity duties which means they don't get done at all.

Know the basics

No matter how excellent a person's qualities and credentials, it doesn't mean they know the cybersecurity basics, since some choose not to pay attention to this topic. Every person is capable of learning, and all need periodic reminders of the basics plus motivational nudges to get them done.

There are smart and capable lawyers who do not know what two-factor authentication is, others who know what it is, but not whether *their* firm employs it on important systems.

Lacking that knowledge is similar to not knowing what a seat belt is or not knowing whether one's seat belt is fastened while riding in a car. It may be a basic part of driver safety, but it is necessary and important.

Solid management of cybersecurity and information systems is equally important and basic, but some have not thought about it, and some do not know if their firm has a cybersecurity program, a written policy, or who might be in charge. That's like owning a car and not realizing that someone needs to maintain it, oil needs to be changed, brakes checked, registration and insurance renewed, and so forth.

When cybersecurity basics don't get done, the people in charge probably were thinking one or more of these:

- If they call it basic, I must already know it.
- If it's basic, we must already be doing it.
- Learning about the basics is below my pay grade.
- Cybersecurity basics are for someone else to deal with.
- We don't have time for that.
- We don't have money for that.

Weigh and decide

To manage means to weigh options and decide. Even lawyers and law firm leaders who excel in managing their litigations, cases, and client matters sometimes neglect to manage certain areas of the firm, and especially so for their information technology systems and cybersecurity.

Too often, firm leaders say:

"Our IT provider is in charge of that."

or:

"I can't make decisions on technology or cybersecurity issues because I don't know anything about them."

Abdicating leadership and management is a mistake, especially for technology and cybersecurity. Lack of subject matter expertise cannot be a reason to avoid the topic.

We already know this is true, because clients come to lawyers to seek legal advice and guidance because the client doesn't know law. The lawyer advises and helps the client make the best decision given the facts, law, and potential outcomes.

Law firm leaders are in a similar position when making decisions on technology. It is not their area of expertise, so they ask questions, investigate, weigh options, seek solid advice from objective professionals in the field, and then make a reasonable decision.

Conclusion

In future columns I'll return with more details on the cybersecurity basics, my Four Pillars of Cybersecurity, and the exciting journey of discovery about your information systems (in other words, "inventory").

Cybersecurity serves the purposes of protection, compliance, and preventing cybercrime and other bad events from happening. Cybersecurity is also a way to take charge of your information technology and systems to get to know them and manage them well.

If you crave unplanned excitement, skip the seatbelt, text while you drive, and neglect to manage your information systems.

When it comes to your firm, remember that cybersecurity is a necessary pursuit. So first follow the mundane path of cybersecurity basics; pursue good management, make solid decisions as questions or issues arise, get to know your systems, and secure them diligently.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the author

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity and better protect and manage information systems. His latest book is "Cyberlaw: Law for Digital Spaces and Information Systems" (2025). His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on April 16, 2026.