Maintain and improve the cybersecurity program of your firm or organization

By John Bandler, Esq., Bandler Law Firm PLLC

FEBRUARY 17, 2026

If your firm has a cybersecurity program in place, then your work is not done because you need to continually maintain and improve it. That's what we cover in this article.

If your firm does not have a cybersecurity program, or you are not convinced about the need for it, consider pausing this read to see my prior column and get up to speed.

Remember the cybersecurity program fundamentals

Let's recap some fundamentals from last time because if you remember them, it allows this article to move you forward.

When organizations do cybersecurity right they also manage their information assets well.

Your firm needs a solid cybersecurity program to protect from cybercrime, comply with laws and professional responsibilities, and help you fulfill your mission of serving clients. Those are my three goals of cybersecurity, which we will revisit soon.

When organizations do cybersecurity right, they also manage their information assets well. This can prevent bad things while making good things possible. There's also a psychological benefit when the nagging anxiety with procrastination of cybersecurity gets replaced by peace of mind when those things are done properly.

Firms with a solid cybersecurity program have active and ongoing management of cybersecurity which includes these components:

- Written policy and plan,
- Cybersecurity basics,
- Management, and
- Training.

See, "Build your cybersecurity program in your firm or organization," Reuters Legal News, Dec. 15, 2025, https://bit.ly/4kBDED4.

If you are not sure if your firm even has a cybersecurity program or cybersecurity policy, you know there is work to be done — whether it exists or not.

If you do not work in a law firm, simply substitute the word "organization."

My main goals of cybersecurity

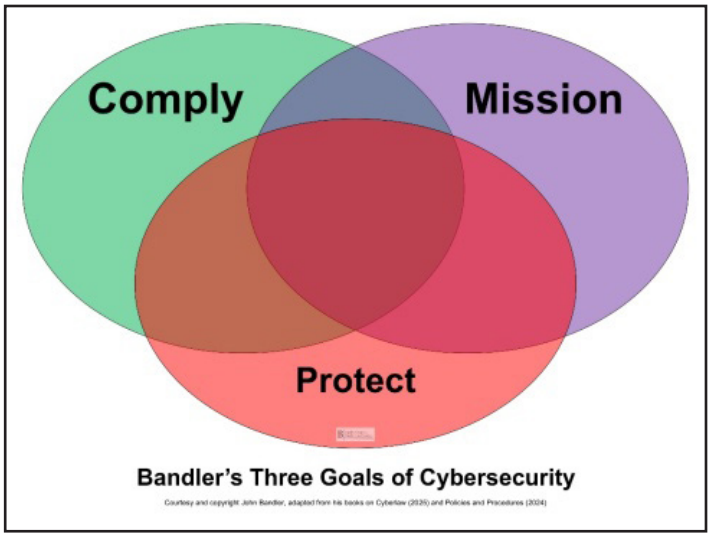
As we periodically seek to improve our cybersecurity program, we revisit those three main goals of cybersecurity which are:

(1) *Protect* from cybercrime,

(2) *Comply* with legal requirements, and

(3) Fulfill our *mission*, including by improving efficiency and the management of information systems.

These three goals overlap as we can depict with this Venn diagram.



There is a fourth goal that is achieved after these three items are properly addressed, and that is *peace of mind* with the knowledge that the right things are being done.

When we embark upon a family road trip, we have some peace of mind if the car is properly maintained and registered, we know the rules of the road, how to drive safely and the route, and we are rested, sober, and attentive.

Policies and procedures should be reviewed annually or sooner if circumstances suggest or require, as periodic review prevents them from becoming forgotten or obsolete.

Similarly, we can obtain peace of mind over our cybersecurity and information systems if we devote sufficient, reasonable time and effort to the fundamentals and know some of the basics are in place.

Continual improvement is the key

Every firm has room to improve.

That's the helpful philosophy to embrace.

Other mindsets can lead to wasted time on defensiveness, deflection, or finger pointing. Cybersecurity is about decisions humans make, and we should also consider how people will react to assessments or critiques of their cybersecurity work.

These questions can cost time:

- Are we compliant with X law, Y regulation, or Z professional responsibility code?
- Are we protected?
- Will we prevent a serious incident?
- Can someone give us a clean bill of health?

They can lead to entrenchment or assertions that everything is "good," both of which can be impediments to improvement.

A better approach is an honest look for priority areas of improvement with a prompt dedication of reasonable resources to achieve those improvements.

If the focus remains on the main goals of the cybersecurity and information governance activities (protect, comply, and mission), then the next questions can be helpful:

- How can we improve our cybersecurity and cybersecurity program?
- What steps should we do first (and now) to improve our cybersecurity?
- How can we improve the management of our information assets?
- How much time and resources are reasonable for us to expend doing this?
- What is the minimum of time and resources we are willing to commit?

This approach allows organizations to accept that continual improvement is needed while recognizing the limitations of life and business. No firm exists just to work on their own cybersecurity and there are reasonable limits to the resources they can expend.

Make sure someone is still in charge of cybersecurity

When you built your cybersecurity program you put someone in charge of it (if you followed my last column). That designation needs to be reviewed because people change, forget, or things get lost in the shuffle.

Very large organizations can hire dedicated personnel to manage cybersecurity, but in smaller organizations that is not possible and a regular employee gets that added duty. You can call this person the "cybersecurity coordinator" or "information security coordinator." This designation needs to mean something, and they need to spend a reasonable amount of time on this duty.

A good cybersecurity policy forms a solid basis for both action and training which means if you are stuck about what to train on, just train about the policy.

Never find yourself in the position of saying or thinking: "Person A is in charge on paper but not really" because that is an admission of a serious transgression.

The person in charge of cybersecurity should also be in charge of maintaining and improving it. They will report to someone higher in the firm, unless they happen to be the highest level of management in the firm. They will need to consult outside resources and can even hire external professionals to assist them in their duties.

Review your written cybersecurity policy and cybersecurity practices

Policies and procedures should be reviewed annually or sooner if circumstances suggest or require, as periodic review prevents them from becoming forgotten or obsolete. A forgotten policy is useless, and an obsolete policy was useless long before anyone realized it was obsolete.

The review of the documents should be done with a review of actions and practices to see what the organization is doing or not and which rules the organization is following or not.

If the organization's actions do not comply with the policy, then the next question is whether the policy needs to be changed, or whether practices need to be changed. When the policy is sound but isn't being followed, the actions need to change. Sometimes circumstances change or the written policy is unrealistic, which requires an update to the document.

The object is to increase the good things that people do, and reduce the bad. Policies are one way to do this, training is another.

Train

Training is simply a way to build knowledge and awareness and can be formal or informal, with many ways to do it.

At a minimum, every member of the firm should know about the cybersecurity policy and what it says. Unfortunately, many firms have people (including leaders) who don't even know if they have a cybersecurity policy or program in place.

A good cybersecurity policy forms a solid basis for both action and training which means if you are stuck about what to train on, just train about the policy.

Take a step forward every now and then

Imagine the question: "*What did your firm do about cybersecurity this year*?"

For some firms, their honest answer would be: "*Nothing*."

Doing nothing is not defensible, and could be equated to not caring at all, and even being negligent or sloppy.

Something needs to be done. That could be an annual review, and some type of improvement. That is the least you should do and allows you to truthfully assert you did *something*.

Even better, do a *reasonable amount* that you can defend and justify, so that you can honestly state that you are reasonable and diligent with cybersecurity.

Skip the worries of procrastination and act today.

You want to expend a reasonable amount of time and resources to maintain and improve your cybersecurity program. You can achieve some peace of mind knowing you have improved your protection from cybercrime, compliance with your responsibilities, and ability to do your job more efficiently.

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 February 17, 2026.