Inventory your systems with the four pillars of cybersecurity

By John Bandler, Esq., Bandler Law Firm PLLC

AUGUST 13, 2026

Let's embark upon a wonderful journey of discovery about our organization's systems to learn what we have, to secure them properly and use them efficiently. This is the scavenger hunt of learning and discovery we mentioned in earlier columns.

We also know it by the simpler (and less appealing) term of an "*inventory*." That term doesn't convey images of joy and fun; it fills some with dread and motivates procrastination. But it is an important process where reasonable steps along this path can result in rewarding progress as you take charge of your information systems.

Why we should discover and inventory

Many components of an organization's information systems are not given a thought until too late. In some cases, this neglect allows incidents to happen, while in others it is a missed opportunity.

If you don't know what you have then you can't secure it and you can't use it efficiently.

Here is the simple takeaway:

If you don't know what you have then you can't secure it and you can't use it efficiently.

If an organization cannot produce a list of its computer devices then it is probably not securing them properly, nor does it know who each computer is assigned to. They would have difficulty reporting them if lost or stolen.

In contrast, a firm that lists and reviews their computers can better secure and manage them. They can assess their age, security configurations, and ponder what would happen if they were lost or stolen, all a process towards improved management and protection.

Some organizations take their digital services for granted until something happens. If they forget to renew the domain registration, or neglect to secure that account adequately, then their website and email can go down. Forget to pay the phone bill and you can lose your phone number, and so forth for every digital service you rely upon.

The brick-and-mortar analogy

The inventory process is similar to how we protect a building from a physical burglary; and both start with the basics.

To secure a building we first review the doors and windows and their locations and how to lock them. Simple and obvious because we know anything unlocked is an easy entry point for the burglar. We also consider that some windows and doors might need a degree of resistance to physical force and tampering. Next, we can consider more complex measures.

To secure an organization's information systems, finding and securing the digital windows and doors means reviewing the digital assets; the computer devices, digital data, online accounts, services and networks that the organization uses. These are virtual entry points for a cybercriminal, and to secure them we first need to identify and locate them. Next comes assessing the relative security of each.

For example, an email account is like a front door. If it has a simple password and lacks two-factor authentication, that's like a door with a flimsy lock that can be easily pushed in, within a high-crime neighborhood where burglaries are rampant, with no surveillance camera, no police department to respond, and no prosecutor to bring charges. Cybercriminals can break in without any fear of investigation, apprehension, or prosecution.

Inventory periodically with the Four Pillars of Cybersecurity

Digital assets should be managed by humans, and a periodic inventory review helps ensure they are secured. Otherwise, they get overlooked for a multitude of reasons (sometimes the organization didn't assign someone to secure it in the first place, people don't get to their task, or leave the organization and their responsibilities don't get reassigned).

Last column we reviewed my Four Pillars of Cybersecurity as a framework to organize and work on cybersecurity. This is a continuous process to:

- Improve *knowledge and awareness* of people in the organization,
- Secure computing *devices*,
- Secure *data*, and
- Secure *networks* and use of the Internet.

This continuous process repeats because cybersecurity is never done. (*See*, "Consider these 4 pillars of cybersecurity as your framework," Reuters Legal News, June 17, 2026, https://reut.rs/3Ss1mYE).

Digital assets should be managed by humans, and a periodic inventory review helps ensure they are secured.

We can organize our inventory along those lines and by focusing on:

- People,
- Computer devices,
- Data and online accounts, and
- Networks.

All of this is a part of building and improving the organization's cybersecurity program to properly manage and secure all aspects of the information systems which we covered in more detail in prior columns.

People and their knowledge and access

Our review starts with people, their knowledge, and their various access to devices, data, and online accounts.

Organizations need to know who all their employees and key contractors are and what electronic access and control they have. All these people need adequate knowledge about the policies of the organization and about safe computing practices. They should also receive an appropriate degree of training each year, properly documented.

Individual services and systems have their own lists of people with access or administrator privileges which needs review. For example, to secure Microsoft Office 365 systems, one needs to know about all of the authorized users and their access. To secure a website, one needs to know who can access it and what changes they can make.

Some managers and leaders make important decisions that affect cybersecurity and information systems, so they need increased knowledge and guidance to help with those decisions, and also need to spend time on cyber governance. The leaders remain responsible if their management — or lack thereof — results in a cybercrime incident or simply inefficient use of existing resources.

Devices

Computer devices include smartphones, tablets, laptops, desktops, and servers. While reviewing these tangible items, you should also include network devices like routers and Wi-Fi access points.

Firms should create and maintain a list of all firm devices, including make, model, serial number, year of purchase, operating system, and who each device is assigned to.

This tracking should start at purchase, through each assigned user, and through end-of-life and ensuring any residual data is securely wiped before sending the device outside of the organization, such as for resale or recycling.

Keep your inventories secure, they are a map of your castle.

This inventory is a starting point and then as time allows the security configurations on each device can be evaluated and improved.

Data and online accounts and applications

Inventorying data is more complex, so resolve to tackle it one step at time.

Our data is everywhere, like a large house that has accumulated things for decades, with cabinets, closets, an attic and basement; some areas unexplored for years.

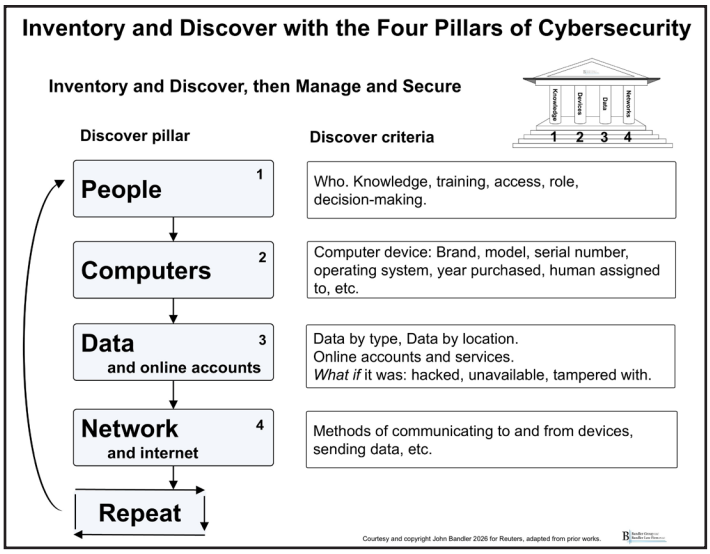
We think about different types of data, and different places the data might be stored.

Types of data include email, documents, spreadsheets, intellectual property, confidential information, contacts, passwords, and personal information of clients or employees.

Places data are stored include devices, servers, external hard drives, cloud-based services such as Microsoft, Google, Apple, Dropbox, social media accounts, and innumerable online accounts with various online services.

Reviewing online accounts is important because those store data and also allow employees and the organization to do things. Lose access — or allow an attacker to gain access — and bad things follow. With the inventory review, organizations can assess potential consequences if certain data (a) was compromised and exposed to a cybercriminal, the world, or an adversary, (b) became unavailable and unusable, or (c) was tampered with.

Once you create an account or purchase a service, that needs to be managed and secured, which starts with the inventory.



Networks and internet

An inventory of networks and internet usage starts with physical network devices (which we may have already done previously with computer devices) and also includes the services and methods through which organization computers and people communicate with each other and the outside world.

This includes Wi-Fi networks, wired networks, internet service, and other mechanisms.

Repeat and refine

Cybersecurity is never complete and is a process of continual improvement, and this is especially true with the inventory, which cannot be done in one sitting. It is important to start the process and take a step. Begin with high-priority basics, then continually improve it over time.

These points help organizations make progress, even in this challenging area:

- The goal is small steps of improvement (not perfection or infinite detail)
- Budget a reasonable amount of time to work on it (*ex.*., 1 hour, 2 hours, 5 hours, etc.)
- Budget a reasonable deadline to take a small step (1 day, 1 week, 2 weeks, etc.).

Periodically review and improve the inventory (at a minimum, each year) focusing on the goals of learning, discovery, and improvement. Keep your inventories secure, they are a map of your castle.

Conclusion

This inventory process aligned with the Four Pillars is a way to discover, organize, and secure your systems. It helps identify the many digital assets in a firm's information systems, and engage people who have a role in managing, protecting, and using them.

Don't let fear or uncertainty hold you back, because that leaves a nagging worry about important tasks left undone. Take a step forward and improve today, learn about your firm's systems, improve how you secure and manage them, and achieve some peace of mind.

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**. He can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on August 13, 2026.