The Document Your Clients Don't Know They Need: a WISP Bridges the Gap between Data Privacy Concepts and Cybersecurity Realities, *New Jersey Law Journal*

November 21, 2025

By: Alfred Brunetti

The following article originally appeared in the New Jersey Law Journal.

Another week, another data breach in the news. In the fleeting moments when not totally consumed with deadlines and meetings, such headlines may cause some business clients to briefly pause to wonder whether they could be next and even ponder if their digital universe is secure enough, but not knowing how to even start to address such concerns, their focus quickly returns to the day-to-day struggles of operations and profitability. For New Jersey attorneys, this creates both a challenge and an opportunity—helping a client translate vague data security concerns into an action item that can actually help secure and improve the business.

Enter the written information security plan (WISP). Not just another compliance document, the WISP is a practical roadmap that turns abstract data protection duties into concrete business practices.

What It Is and What It Does

A WISP is a foundational document that translates data security policy principles, as well as some relevant data privacy tenets, into operational practices by detailing an organization's actual data security processes and controls. Think of it as the operating manual for data security. Done right, a WISP serves two central purposes. First, it satisfies the documentary requirements scattered across privacy laws and regulations. Second, it creates accountability. So, when your client's bookkeeper gets a suspicious wire transfer request, the IT manager needs to decide about remote access authorizations, or a teammate sheepishly admits that he entered his login credentials into a now-suspicious-looking document sharing request portal, the WISP provides the framework for taking decisive and responsive action consistently.

A typical WISP will include provisions that set out responsibilities (for oversight and governance); controls (both administrative and technical, often with reference to separate SOPs for physical measures); risk assessment (on a structured and tiered system); and breach response (the when-it-goes-wrong playbook). The WISP should live with the IT department, but must be a living document that is created collaboratively with input from all stakeholders who play any substantive role in business operations. Purposeful collaboration helps to make sure the plan considers and addresses the unique needs and contours of each business so that it does not merely become a document that exists, but one that is actually used.

For the perpetually liability-minded among us, here's a key point: a solid WISP can be evidence of reasonable care. When negligence claims arising from a data security incident or breach turn on whether security measures were in place and

reasonable, a well-considered and properly implemented plan can be the difference between a defensible case and a real problem.

Why Now Is the Time for a WISP

In the ever-expanding digital ecosystem and electronic marketplace, businesses face obligations from a variety of regulators and influences to keep, at least, the most common data security threat vectors and risk factors at bay. These obligations flood in from all directions.

Nationally-scoped, sector-specific laws and regulations, *e.g.*, HIPAA for certain health information; GLBA for certain financial information; and model laws like NAIC Insurance Data Security for insurance licensees, command attention from businesses in those highly-regulated industries. The activities of some federal agencies, like recent enforcement actions and official statements by the FTC, have emphasized that inadequate data security practices could constitute unfair trade practices. Add to that stew the contractual obligations which permeate nearly all business relationships. Such contractual ties often include operational necessities (like affirmative representations to cyber insurance carriers so that their increasingly stringent underwriting demands can be met) as well as assertions made in the business-to-business context, seen most commonly in the form of data processing addenda or similar provisions that require detailed warranties about the status and maturity of a company's data security practices.

Now salt in the fact that some states, like Massachusetts, expressly require a WISP for any company that deals with the personal information of its residents, while other states (namely many of the nearly 20 which have more recently enacted 'comprehensive' data privacy laws) impose an obligation to have “reasonable” or “appropriate” security measures in place. For example, the New Jersey Data Privacy Act (NJDPA)—which became enforceable in January—and its near-final attendant regulations, require certain businesses that collect or process the personal data of Garden State residents to establish and maintain administrative, technical, and physical data security practices aimed at protecting the confidentiality, integrity, and accessibility of such data. The NJDPA, and similarly equivalent state-specific 'comprehensive' regimes, thrive at telling businesses what to protect, but they are often far less helpful on the all-important how component of data protection.

What results is a dynamic and challenging complexity which demands clarity, accuracy, and good management to ensure not only that express obligations are met but also that essential business functions can be enabled rather than hindered.

Where to Begin

Inventory and Understand. Logically, it's hard to protect what you don't know you have, and even harder to anticipate something you don't understand, so a vital first step is for a business to assess—and document—the types of information and personal data it accesses during its normal operations and to understand how such data moves both within and out of its systems. For many businesses, especially of the small and mid-sized variety, this assessment exercise will reveal some previously unknown data categories and flows, forgotten share files and archive locations, and even some shadow IT tools or functionalities. Reliably and accurately documenting these data types and flows will reveal what needs to be protected.

Roles and Controls. Who can access what and under what controls and circumstances? This is a pivotal question when evaluating the security of any system, whether digital or physical. Even the most advanced vault is useless if everyone has the combination. Role-based access controls will ensure that only position-appropriate individuals gain access to certain systems and only when such access is required to perform an authorized function. A thoughtful and unified procedure that includes a business' human resources and vendor management stakeholders will ensure that once employment or duty status changes, the afforded access will be re-evaluated automatically and correspondingly changed. Authentication controls and protocols (in the form of password policies or multi-factor authentication requirements or the like) will aim to make sure that commonly-guessed credentials or an unattended workstation or laptop do not leave the system open to prying eyes or an outright attack. Balancing security with operational realities is key here, so before imposing absolute restrictions, be sure to evaluate the resulting impacts and benefits.

Plan and Train. Although all parts of a WISP are important, the incident response portion is likely the most valuable and a frequently underserved section. Properly drafted, it will inform the business of what to do, step by step, when a breach or data security incident occurs. It will be the playbook that clearly and practically dictates who's in charge, how incidents get assessed, when to engage outside counsel and technical experts, what notification obligations need evaluation, and how operations should continue. Decisions made in the first hours following an incident strongly impact the likelihood of whether a business will face regulatory sanctions, class actions, or devastating reputational damage. Because the stakes can be so high, a regularly updated and pressure-tested playbook is a tremendous mechanism to lean on for the steady direction and guidance needed during an event as impactful and disruptive as a security incident. That said, even the best drafted plans are worthless if no one knows they exist or how to confidently implement them. The WISP itself should mandate regular security awareness training, tailored to the practices that pose the greatest risk to the particular business. Such trainings are best when they clarify expectations, obligations, reporting channels and actual actions—affirmative and responsive—that an employee or representative should take in specific circumstances.

Moving Forward

Most business clients want to do the right thing, but in the often-confusing world of technology, it can be difficult to know what that is. As privacy and security obligations expand, WISPs will only grow in importance. For New Jersey practitioners, understanding them isn't niche expertise anymore—it's fundamental knowledge for advising clients on operational risk, regulatory compliance, and business development.

A well-thought-out plan provides the structure that is needed to transform security from an IT pain point or emergency into an actionable and practical company-wide responsibility. Help your clients design this vital document before they're forced to explain why they never had one.