The lawyers at Foley & Lardner have a message for IT pros about BYOD: Resistance is futile!

That's not an exact quote but it's pretty close. The firm's IT and outsourcing practice recently conducted a webinar for companies grappling with employee-owned devices on and off their corporate networks and the long list of potential issues the BYOD model can cause.

Naturally, the event focused on the legal and related risks associated with BYOD. But it wasn't doom and gloom. The lawyers highlighted the positive potential outcomes of allowing employees to use their own mobile devices and other hardware at work, such as lower costs, improved employee productivity and satisfaction, and even hiring -- the presentation cited a Unisys report that found 44% of job hunters find an offer more attractive if the employer supports iPads. The bottom line: BYOD is happening whether you like it or not.

"At the end of the day, BYOD is not going anywhere," said Foley & Lardner partner Matthew A. Karlyn. "It's only going to increase."

That said, there are innumerable risks associated with allowing employees to use their personal smartphones, tablets, and other hardware for company business. Just as the head-in-sand strategy would be ill advised, so too would BYOD anarchy. Karlyn and his colleagues stressed the need for a strong, thorough policy that employees can actually understand. To that end, he advised regular education and training initiatives, both in person and online. Finally, he noted that policies must be enforced with meaningful consequences for rule-breakers; otherwise, rules are essentially worthless.

The lawyers noted that policy, training and enforcement specifics will vary by business. Highly regulated industries like healthcare and finance, for example, have an entire other set of concerns related to BYOD. But they highlighted just how complex the BYOD workplace can be -- and how specific your policy must be as a result.

A fundamental idea behind the policy-education-enforcement strategy is that the legal and other risks of BYOD can be reduced if both employer and employee clearly understand those risks and their roles and responsibilities in managing them. Consider these six specific issues that you and your employees might not be adequately addressing.

### 1. Data Is Discoverable.

Foley & Lardner partner Michael R. Overly began his part of the presentation by noting that BYOD devices might be discoverable in lawsuits. In English: Everything an employee does on her personal iPhone, for example, could be used as evidence in a lawsuit against her employer. Overly said that usually comes as a surprise to senior management when he does corporate
training work. "More times than not, those executives are absolutely, positively astonished when we explain that when someone participates in a BYOD program, that device may be subject to discovery in litigation," he said.

Employees who assume they have a right to privacy -- it's "my" device, after all -- might likewise be in for a shock. The personal devices they use at work could be examined not only by their employer but by the other party in the lawsuit. Their social media, photographs, personal email, geo-location information and many other kinds of data could be pored over at length.

"Even though people may understand [the discovery process] in a general sense, [they] do not appreciate just how invasive a review like that can be," Overly said. "Which is why it's so important to make sure that people that elect to participate in a BYOD program understand that type of risk -- that, by participating, you're giving up certain rights."

2. Discovery Can Be Expensive.

If you have a come-one-come-all approach to BYOD -- as in "if we allow one device, we might allow them all" -- this might make you rethink it. Lawyers don't typically work cheap and discovery can get expensive. If employees are using not just one but two or more personal devices for work, you're potentially adding a multiplier to your legal costs in a lawsuit. That's because all of those devices might have to be turned over for discovery. In fact, there doesn't even need to be a lawsuit to incur such costs -- just the threat of one and a requirement for litigation hold. "This is a cost that needs to be built in and understood in connection with deciding whether a BYOD program is appropriate for your business," Overly said.

3. BYOD Devices Are Subject To Border Search And Seizure.

If you've got employees that travel internationally, their devices might be subject to search or seizure at border control -- something they need to be aware of in advance if they're going to use their own when they're on the road. This falls into the category of employee awareness. They need to know, via policy and education, that they're forfeiting certain rights to their personal devices by using them for work.

4. Who's Responsible For Repetitive Stress Injuries?

Employers can manage the costs and risks of an employee getting hurt on the job in a variety of ways: Insurance, safety training, ergonomic office equipments and so forth. This would include desk-bound employees who develop repetitive stress injuries from typing, mousing or similar tasks. But what if they get "BlackBerry thumbs" from a device they own? Can they take action against their employer? If you think that sounds far-fetched, think again: Overly said they have already seen two cases where an employee at least explored a claim against their employer as result of using a personally owned device. "This is another policy and training thing: By putting employees on notice that there are issues, particularly repetitive-stress issues, with regards to the use of technology," employers can limit their liability, Overly said.

5. The Demise Of The Great American Novel.
BYOD discussions tend to focus on the hardware that made it famous, namely smartphones and tablets. But bring-your-own can include laptops, netbooks, ultrabooks and other gear -- something bound to increase if Windows 8 hardware proliferates. Overly noted a situation involving a person who alleged that his employer deleted files from a personal laptop after he brought it to the office to have security software installed. Those files included the only copy of the novel he'd been writing for years; the claim stopped just short of court. Again, this scenario -- the responsibility for loss of data on an employee-owned device -- can be proactively managed via policy, provided the employee is made aware of the risks. (That particular employee might also need a tutorial on the many low-cost options for backing up files.)

5. What Happens When An Employee Shares A Device?

A strong BYOD policy would protect the company in the case of the employee's deleted novel-in-progress. It would not do the same if that novel was written by the employee's spouse. If you've ever shared or borrowed a computer, tablet or phone with family or friends, this one's for you. Overly called shared use of employee-owned devices one of the most pressing BYOD issues around, in part because it can't be easily mitigated with policy. An employee sharing a BYOD-use iPad with his spouse certainly opens up potential issues such as corporate data loss or security breaches. But it also creates a much thornier problem in terms of potential legal action against the employer. Overly described a case in which a spouse used a BYOD device to photograph an important, one-time life event. The company, in the course of routine device management, later deleted all of the photos -- the only copies -- via remote wipe. "How does the company protect itself against a claim by that spouse?" Overly said, noting that the employer doesn't have any policy or contract with that person governing use of the device. "It's very, very difficult to do," he said. The total separation of personal and business data on employee-owned devices is "the holy grail" for BYOD shops, Overly added.

6. What About When An Employee Gets Rid Of A Device?

Employees that sell or recycle a BYOD device after upgrading pose another risk, as do lost or stolen devices. A common policy and technology strategy is to enable remote wiping of the device's data and require it as a condition of program participation. Like most protections, remote wipe is not fool-proof. But it's a key tool in managing the downside -- which can be steep simply because of the sheer volume of devices. Device disposal occurs millions of times when Apple releases a new iPhone, for example, or more incrementally when people accidentally leave their phones in taxicabs or airport waiting areas. Employee termination is another scenario where remote wipe can be crucial.

"Terminated employees [are] always a challenge because they may not be interested in helping the company with anything," Overly said.