New law protects trade secrets

President Obama has signed a new federal law that expands the ability of companies to sue when someone steals or misuses a trade secret.

The law also contains new requirements for employment contracts that refer to trade secrets – which means that many such agreements should now be revised.

The "Defend Trade Secrets Act," or DTSA, will change the legal landscape by making misuse of trade secrets a federal issue, comparable to patent, trademark and copyright infringement.

In the past, each state has had its own rules for trade secrets. In all but three states (Massachusetts, New York and North Carolina), these rules were based on something called the "Uniform Trade Secrets Act." But while the act has the word "uniform" in the title, it really isn't all that uniform because each state has adopted a number of variations on it.

The new DTSA doesn't replace the current state laws, but it does give companies an alternative way to take action if an employee, a former employee, or a competitor misuses confidential business information.

There are two big advantages to DTSA. One is that it allows a company to sue in federal court, regardless of where the parties live and how much money is at stake. This is new, and federal court can provide a number of advantages. For instance, a federal suit eliminates the extended squabbling that can often happen in these lawsuits over which state's law should apply.

The other advantage to suing under DTSA is that a business can, in some cases, get a court to authorize the immediate seizure of property necessary to prevent a trade secret from being divulged or exploited – without first informing the other side.

To do this, a business must (1) show that it's likely a trade secret is being misused, (2) specifically describe the property and where it's located, and (3) show that if the other side were tipped off in advance, there's a good chance it would destroy, move or hide the property.

After a seizure, there must be a hearing within a week. If it turns out the seizure was invalid, the other side can sue for any damages.

These kinds of "secret" or "gotcha" seizures are currently available in cases involving trademarks and copyrights, but this is the first time they have been allowed in trade secret cases.

DTSA doesn't specifically say what kinds of property can be seized. In trademark and copyright cases, it's the infringing goods or evidence of infringement. In DTSA cases, presumably, it could include documents, cell phones, computers, e-mail servers, or even products created using a trade secret.

The law applies to any trade secret misappropriation that occurs after May 11, 2016.

A separate part of DTSA says that people can't be sued under the law for revealing a trade secret if they do so (1) as a "whistleblower," when reporting a suspected violation of the law to the government, or (2) as part of a lawsuit against their employer, if they reveal the secret to the court but not the public at large.

Further, businesses must notify employees, consultants and contractors of their right to reveal trade secrets in these two situations as part of any employment agreement that refers to trade secrets and that's entered into after May 11. This includes hiring agreements, separation and severance contracts, non-compete agreements, and some parts of employee handbooks.

There's no monetary penalty for not including this notification, but a company that doesn't include it and then sues someone under DTSA won't be allowed to collect punitive damages or force the other side to pay its attorney fees. This deprives a business of significant leverage it could use to settle a case, so it's a good idea to make sure the language is included.

Federal penalties are increasing dramatically

The maximum penalties that can be imposed on businesses by federal agencies are being dramatically increased, as a result of a new law passed by Congress.

OSHA's civil penalties hadn't increased since 1990, but that changed on August 1, 2016, when they jumped roughly 80%. The top penalty for a serious OSHA violation went from $7,000 to $12,471, and the top penalty for a willful or repeated violation went from $70,000 to $124,709. What's more, if an employer was inspected before August 1, but OSHA didn't issue a citation until after August 1, OSHA can issue a penalty at the new higher rate. Since OSHA has six months from the date of a violation to issue a citation, it's expected that a lot of companies that were inspected in the first part of 2016 will see large penalties assessed after August 1.

Also on August 1, the maximum penalty for an I-9 paperwork violation went from $1,100 to $2,156. The maximum first-offense penalty for knowingly hiring an unauthorized worker went from $3,200 to $4,313.

The maximum penalty for willful or repeated violations of the wage-and-hour laws increased from $1,100 per employee to $1,894 per employee. And a number of EPA penalties have gone up as well.

Drug testing policies may need to be revised

If you have a policy that requires drug testing after a workplace accident or injury, you may need to change it as a result of new rules issued by OSHA.

The new rules generally require that companies have a reporting procedure in place for work-related injuries and illnesses, and prohibit them from discouraging workers from reporting injuries. The catch is that, according to OSHA, a policy that requires drug testing after a workplace accident could discourage workers from reporting accidents in the first place.

To be clear, OSHA is not saying that you can *never* give a drug test after a mishap. But to justify a test, two things must be true:

- There must be a reasonable chance that drug use was actually the cause of the injury or accident. So a drug test wouldn't be okay if an employee reports a repetitive strain injury, for instance, or if an accident was due to an equipment malfunction.
- The drug test you use must be able to determine if the employee is impaired *right now*. A drug test that can only show whether an employee was impaired at some point in the recent past isn't good enough.

It's a wise idea to review any drug testing policy you have in place and make sure it complies with the new rules.

Many computer 'hacks' are actually low-tech thefts

All businesses are scared these days of having their data stolen by highly sophisticated foreign computer experts – and yet a surprisingly large number of "hacks" are actually very low-tech affairs, carried out by people with minimal computer skills. The good news is that some simple measures can reduce the risk.

According to a study by the Ponemon Institute, the vast majority of CEOs view sophisticated intentional hacking as the biggest data security problem they face. The vast majority of IT managers, on the other hand, see the biggest threat as careless employees who haven't received basic security training about phishing, passwords, cloud access, and the like.

To take one example, you might have heard that a St. Louis Cardinals baseball team employee was recently sentenced to jail for hacking into the computer secrets of a rival team, the Houston Astros. But you might not know exactly how he did it.
When two Cardinals employees left to go to work for the Astros, manager Chris Correa required them to turn over their Cardinals laptops and tell him their passwords.
When Employee #1 arrived at the Astros, he used a computer password that was almost identical to the one he used with the Cardinals. Correa was able to guess the password and get into the Astros' system.
When the Astros suspected something was up, they sent an e-mail to all employees requiring them to change their passwords. The e-mail contained a temporary password that employees could use to access the system and create a new password.
You guessed it – Correa found the e-mail that went to Employee #1. Then he used the temporary password to get into Employee #2's account and steal even more data.
Prosecutors claimed Correa caused the Astros losses of $1.7 million. And a simple requirement that new employees choose a password that's very different from the one they used with a previous employer could have prevented this very low-tech, low-skilled attack.

What happens to unused 'flexible spending' funds?
Many companies have flexible spending accounts that allow employees to pay health care and dependent care expenses with pre-tax dollars. The biggest drawback to these accounts is that they're "use it or lose it" – so if employees put money into an FSA and don't spend all of it on qualified expenses during that calendar year, they forfeit the remainder.
So what happens to the money they forfeit?
The short answer is that the business can simply keep it. However, if a business wants to ease the burden on employees and make the FSA a more attractive benefit, there are several other options allowed under the tax laws:

- A company can give employees a grace period of up to two and a half months. So if employees don't spend their whole FSA balance in a calendar year, they can be given up until March 15 of the following year to use it up.
- For health care plans (but not dependent care plans), a company can allow employees to carry over funds of up to $500 from one year to the next. However, if you allow employees to carry over funds, you can't also allow them a grace period – you have to choose one or the other.
- A company can combine all the forfeited funds and use them to give all employees a "sale" on the next year's contributions. So for instance, employees who contribute $450 to the plan the next year might be credited with $500 in their account. This must be done on a "reasonable and uniform" basis, so all employees are treated the same. As an example, this means you can't give a bigger discount to employees who had a larger amount of unused funds the previous year.
- A company can also use the combined funds to make contributions to employees' accounts the next year without regard to how much the employees themselves contribute. Again, this must be done on a reasonable and uniform basis.
- Finally, a company can return the unused funds to the employees. However, it can't simply give back the unspent funds. Rather, it must collect up all the forfeited money and then give it to *all* plan participants in proportion to how much they contributed the previous year – *not* in proportion to how much was left in their account at the end of the

year. And this reimbursement will be considered taxable wages to the employees for the year in which the reimbursement was made.