Kevin Cloutier

Cybersecurity Measures to Protect Employers' Confidential Information and Trade Secrets

by Kevin Cloutier, Shawn Fabian, Mikela Sutrina, and Amy Harwath, Sheppard, Mullin, Richter & Hampton LLP

This practice note provides guidance on cybersecurity measures available to employers to protect their confidential information and trade secrets.

Specifically, this practice note covers the following key issues:

- What is cybersecurity?
- What types of information constitute trade secrets?
- What are the key preliminary steps to support an employer's cybersecurity program?
- What are key cybersecurity initiatives employers should take?
- Who should be involved with oversight of trade secrets within a company?
- What are the best practices for planning for (and responding to) a theft/loss of trade secrets due to employee conduct?
- What cybersecurity precautions should an employer take for employees who resign or are terminated?
- What issues may arise when a data breach involving trade secrets occurs?
- What are the benefits of bringing claims under the Computer Fraud and Abuse Act?

This practice note does not address (1) protecting personally identifiable customer information, (2) sector-specific regulatory requirements, or (3) obligations to third parties (e.g., vendors, co-venturers, clients).

For information on the use of restrictive covenants to protect trade secrets and confidential information generally, see the Restrictive Covenants practice notes page. For additional practice notes concerning trade secrets, see the Protecting Trade Secrets practice note page. For information on state laws on protecting trade secrets and confidential information, see Chart – State Practice Notes (Non-competes and Trade Secret Protection). Also see Chart – State Expert Forms (Non-competes and Trade Secret Protection) [ADD LINK]. For more information on dealing with trade secrets and confidential information protection upon termination, see Trade Secrets and Confidential Information Protection upon Termination Checklist. For more information on protecting confidential information at hiring, see Trade Secrets and Confidential Information Protection upon Hiring Checklist.

What Is Cybersecurity?

In the digital age, employers store most information on computer systems and networks. Cybersecurity refers to the technological protection of computers, networks, programs, and systems from attack, damage, and unauthorized access.

Cybersecurity is particularly important for employers because they maintain a wide variety of confidential information on computer systems and networks that they must protect not only from data breaches that anonymous hackers cause, but also from trade

secret misappropriation that their own employees commit. Employers must protect their trade secrets because trade secrets provide employers with commercial advantages over their competitors.

Benefits of Establishing a Workplace Cybersecurity Program

Establishing and maintaining formalized workplace cybersecurity programs can help minimize the risk of trade secret misappropriation by reducing opportunities for unauthorized parties to gain access to an employer's networks, computers, and data. Employers with a well-established cybersecurity program are also better positioned to respond and recover faster in the event of a data breach or trade secret misappropriation. Recovery speed is significant because it shows the employer has an important and protectable interest, which it must demonstrate to a court to establish a trade secret misappropriation claim. Additionally, faster recovery allows an employer to mitigate and limit the damage that may result from a data breach.

Variations of Cybersecurity Measures among Different Types of Employers

Cybersecurity measures are unlikely to vary significantly based on the type of information that an employer seeks to protect. While a manufacturing company will have different types of trade secrets from a retail company (e.g., blueprints of machines versus customer lists), the electronic storage of trade secrets via a computer, software system, or other online repository means it is possible that they can each be protected by the same or similar cybersecurity methods.

However, the size of the employer may determine what kinds of cybersecurity measures are appropriate for a particular employer. Certain small companies may have fewer resources and personnel than large companies. This means cybersecurity oversight may rest with one or a few individuals rather than an information security team, for example. Small companies may also not have the financial resources to invest in information technology or to install many types of software and programs to protect their computers and network. That does not mean that a court will find that smaller companies fail to take reasonable steps to protect their trade secrets. For example, at least one court held that keeping customer files in a closed file drawer, informing employees that files were confidential, and limiting employee access to the customer files were "reasonable for a small tailor shop to maintain the secrecy of a customer list and customer information." Elmer Miller, Inc. v. Landis, 253 Ill. App. 3d 129, 134 (Ill. App. Ct. 1993).

Regardless of size and resources, employers should use as many of the cybersecurity measures described below as possible in the event they must demonstrate to a court that they took reasonable steps to protect their trade secrets.

What Types of Information Constitute Trade Secrets?

As a threshold matter, employers must identify what types of trade secrets warrant protection before it can implement protective measures. Protective measures may differ based on the nature and value of the trade secret being protected. Employers may protect electronically stored trade secrets using the cybersecurity measures described below. It is within an employer's discretion to determine on a case-by-case basis the nature or extent of cybersecurity measures to provide for its trade secrets or other confidential or proprietary information, depending on the degree of its value to the business.

There are many types of trade secrets that employers may electronically store that are subject to cybersecurity measures, including, but not limited to:

- Customer or potential customer lists
- Employee lists
- Employee agreements or other information regarding wages or benefits
- Cost, price, billing, and profit information and methodology
- Marketing and business plans
- Customer service and supply preferences or requirements
- Designs, formulae, recipes, and computer code
- Contracts and contract negotiations –and–
- Databases and spreadsheets containing logistical data and statistics

Statutory Definitions of Trade Secret

Employers alleging trade secret misappropriation must first prove the misappropriated property was a "trade secret" as defined under most state Uniform Trade Secret Acts (UTSA) (or other local trade secret statutes) or the Defend Trade Secrets Act of 2016 (DTSA), 18 U.S.C. § 1836. See Trade Secret Fundamentals. For additional detail on the DTSA, including, among other things, an analysis of available DTSA remedies, see Eric E. Bensen on the Defend Trade Secrets Act, 2016 Emerging Issues 7433.

UTSA § 1.4 defines trade secret as:

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
>
> Unif. Trade Secrets Act § 1(4).

The DTSA provides a similar definition of trade secret:

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

18 U.S.C. § 1839(3).

The measures an employer takes to protect confidential information and data may determine the extent of legal protection afforded to their trade secrets. Both the UTSA and DTSA require employers to make "reasonable efforts" or take "reasonable measures" to keep information confidential for such information to qualify as a trade secret. What constitutes a reasonable measure may depend on the type of trade secret being protected. As described below, reasonable efforts usually consist of a combination of security measures.

Note, however, that the DTSA provides a carve-out that immunizes from liability under both federal and state trade secret law an individual's disclosure of a trade secret:

- To the government or to an attorney for the purpose of reporting or investigating a suspected violation of law –or–
- Made under seal in a court filing

18 U.S.C. § 1833(b).

The DTSA requires employers to either provide notice of this immunity in their confidentiality agreements or cross-reference a policy document that explains its reporting policy for suspected violations of law. Id. A federal court in Massachusetts, interpreting the DTSA immunity provision, treated it as an affirmative defense and required the party asserting it to support it with factual evidence. See Unum Grp. v. Loftus, 2016 U.S. Dist. LEXIS 168713 (D. Mass. Dec. 6, 2016). See also Defend Trade Secrets Act (DTSA) Case Tracker.

What Are the Key Preliminary Steps to Support an Employer's Cybersecurity Program

To properly support its cybersecurity measures, the employer should engage in the following preliminary steps.

Provide Notice to Newly Hired Employers on Confidential Information and Trade Secrets

Employers should inform newly hired employees at the outset of their employment that they will have access to confidential information at the beginning and/or during the course of their employment. Employers should strongly consider setting forth the categories of confidential information to which the employee will have access. The best practice is to provide this notice and receive an employee's acknowledgment of it. This notice serves to protect against misappropriation because it prevents employees from later claiming a lack of knowledge as to the existence of a trade secret(s).

Have Employees Sign Confidentiality Agreements

Confidentiality agreements, also known as non-disclosure agreements, set forth what types of information the employer considers confidential, the employer's policy against improper use or disclosure of such information, and the consequences of violating the employer's confidentiality policy. See Confidential and Proprietary Information and Inventions Agreement and Understanding, Negotiating, and Drafting Non-disclosure Agreements on Behalf of Employers. For information on state laws concerning confidentiality agreements and other restrictive covenants, see Chart – State Practice Notes (Non-competes and Trade Secret Protection). Also see Chart – State Expert Forms (Non-competes and Trade Secret Protection).

Employers may provide the confidentiality policy in a non-disclosure agreement, an employee handbook, or a stand-alone policy issued with new-hire or onboarding paperwork, or conspicuously post the confidentiality policy in the workplace (or make it available through a combination of some or all of the above methods).

Counsel should be aware that these agreements serve as evidence of notice to employees and their consent to the employer's confidentiality policy. An employer can use such agreements to demonstrate to a court that it took reasonable steps to protect its confidential information and trade secrets.

Develop Information Security and Confidentiality Policies

Employer policies should prohibit employees from downloading, duplicating, altering, removing, deleting, or installing data, files, passwords, and programs without prior written authorization from the individual(s) or committee in charge of information security (or a high-level administrator and/or executive depending on the personnel employed by the company). Policies should also prohibit employees from sharing accounts or revealing passwords, since individualized and unique log-in credentials ensure that only those employees with authorization can access confidential information.

Policies are an important step in maintaining the secrecy of confidential information because they may constitute notice to employees. Indeed, courts have denied affording trade secret protection to employers who failed to have written policies governing confidentiality and trade secrets. See CMBB LLC v. Lockwood Mfg., Inc., 628 F. Supp. 2d 881, 885 (N.D. Ill. 2009) (holding that an employer did not take reasonable steps to maintain the secrecy of its customer information where it failed to inform employees that its customer information was a trade secret or considered confidential). The court reasoned that the employer did not have any written agreements or policies limiting the use of customer information, did not mark hard copies to indicate their confidentiality, and did not have a written policy or procedure as to what individuals who left the employer were to do or not do with customer information. Id.

In addition to non-disclosure and confidentiality agreements with individual employees, employers should also have established precautions, policies, and practices in place when sharing confidential information and data with third parties. For instance, a court held that an employer made reasonable efforts to maintain the secrecy of its computer software by restricting access to its programmers and to third parties who had licensing agreements with it and requiring key employees who had access to the software to sign confidentiality agreements. Liberty Am. Ins. Grp., Inc. v. WestPoint Underwriters, L.L.C., 199 F. Supp. 2d 1271, 1286 (M.D. Fla. 2001). For more information on confidentiality policies, see Crafting Confidential and Proprietary Information Policies and Confidential and Proprietary Information Policy.

Key Aspects of Information Security Policies to Reduce the Risk of Trade Secret Misappropriation/Loss

To help minimize the risk of trade secret theft, an employer's information security policy may set forth, among other things, restrictions and requirements on:

- Using the employer's electronic resources to disclose confidential information, including bring-your-own-device (BYOD) restrictions
- Storing confidential information on the local or hard drive of any computer or any portable storage device, including personal devices
- How long confidential information may be stored on a portable device
- Ensuring confidential information stored on a portable device will be encrypted and deleted upon completion of the business need
- Internet use and access to personal e-mail accounts using the employer's network or server system
- Downloading, duplicating, altering, removing, deleting, or installing data, files, programs, passwords, or other applications

- Accessing the company's network and information on non-secured Wi-Fi
- Sharing or revealing account information and passwords
- Reporting any violations of company policy or potential security breaches

Employers should also reserve the right to inspect, investigate, or search an employee's files and messages by accessing the employee's work devices, voicemail, and e-mail accounts, and overriding any passwords and access codes to the employee's work devices and accounts. Employers should also remind employees that work devices are the employer's property, and that employees should have no expectation of privacy with respect to communications on these devices.

Conduct Employee Training on Maintaining Trade Secrets

Employees, particularly those who have access to trade secrets, should receive training as to the importance of maintaining the secrecy of such information and how to properly maintain the trade secrets. Training arms employees with the knowledge and skills necessary for use and compliance with the employer's cybersecurity measures and policies. An employer's efforts to train its employees on how to handle confidential information can be part of its demonstration to a court that it has taken reasonable steps to maintain and protect its trade secrets. See, e.g., Autonation, Inc. v. Peters, 2016 U.S. Dist. LEXIS 57373, at *11 (S.D. Fla. Apr. 29, 2016) (holding an employer made reasonable efforts to maintain the secrecy of its trade secrets where it held specialized training sessions for employees, stored its information in a password-protected central system, and required employees to sign confidentiality agreements).

Cybersecurity Insurance

Cybersecurity insurance is beneficial because it provides financial protection in the event of a cyberattack, including:

- Coverage for data breach liability
- Expenses such as forensic fees and response costs incurred in dealing with a data breach
- Loss of income attributable to the breach
- Defense costs –and–
- Fines and penalties

An insurance provider may also provide resources for employers that join its network, such as breach management expertise and staff support. Additionally, insurance companies may require insureds to meet a certain standard of security, which may aid the employer in demonstrating to a court that it took reasonable measures to protect its confidential information.

However, there are several risks employers should contemplate when considering cybersecurity insurance. If the insurance coverage requires insureds to use the insurer's own breach management team, employers lose control over making key business decisions relating to their data breach response.. This can be particularly significant where the employer is in a specialized industry, where people with knowledge and experience in that industry are best-equipped to make these decisions. Additionally, it may not be worth filing a claim for every security breach, no matter how minor. Employers should also be mindful of the fact that, as in other insurance contexts, the premiums they pay may be more than the payouts they receive under their policies when it comes to making a claim. Relatedly, insurance companies may charge higher premiums to high-risk companies, such as those with a history of data breaches. Some employers also may not closely enforce their own cybersecurity policies if they feel their cybersecurity insurance can provide a sufficient safety net.

Whether an employer should get cybersecurity insurance is a question each employer must answer for itself, and every employer should carefully examine this issue.

What Are Key Cybersecurity Initiatives Employers Should Take?

Develop Identity and Access Protection

Employers can take several measures to ensure only those employees with proper authorization have access to confidential information. Limiting access to only those with authorization demonstrates that the employer is not widely disseminating its confidential information, thereby keeping it as secret as possible. Such limited-access measures include, but are not limited to, (1)

individualized and unique log-in credentials to certain files, programs, or software; (2) password protections; and (3) restrictions on access.

Individualized and Unique Log-in Credentials

Because employers often keep confidential information in a computer program or system, there must be a method to ensure that only authorized employees will have access to it to maintain secrecy. Individualized and unique log-in credentials act as a means of identity verification so that only those employees who are meant to access confidential information can do so. See, e.g., Arminius Schleifmittel GmbH v. Design Indus., Inc., 2007 U.S. Dist. LEXIS 10847, at *3 (M.D.N.C. Feb. 15, 2007) (employer took reasonable efforts to maintain the secrecy of its library of customer information where only employees who held a unique log-in and passcode could access it).

Password Protection

Solely using passwords to control access to trade secrets may not constitute a "reasonable step" in protecting such secrets, but it is an important and basic step. Effective password-protection policies require employees to change their passwords periodically and to use passwords that meet minimum strength and recycling requirements. Strength requirements make passwords difficult to guess. Recycling requirements provide an added layer of protection in case an old password ends up in the wrong hands. See VAS Aero Serv., LLC v. Arroyo, 860 F. Supp. 2d 1349, 1353 (S.D. Fla. 2012) (where an employer took reasonable efforts to protect confidential information contained in its databases by, among other things, permitting only key employees to access the databases, requiring authorized users to change their log-in credentials every 90 days, and mandating authorized users to select a password that was at least seven characters long and contained both letters and numbers).

Need-to-Know Access

Employers should limit electronic access to trade secrets to only those employees who require the information to perform their job duties. Limiting access on a need-to-know basis demonstrates that an employer believes its information is secret, thereby warranting trade secret protection. Employers should use software that controls log-in credentials and restricts the type of information to which employees have access based on their management level, security authorization, and/or job duties. See, e.g., Uhlig LLC v. Shirley, 2012 U.S. Dist. LEXIS 99387, at *7 (D.S.C. July 17, 2012) (employer provided sufficient evidence that it used reasonable efforts to maintain the secrecy of its trade secrets where it required network passwords and restricted access to certain information depending on the employees' job functions).

Develop Policies Restricting Employee Use of Portable Storage and Mobile Devices

Digital information can be taken, and malware can be introduced, through portable storage and mobile devices, including, but not limited to:

- Smartphones
- Tablets (e.g., iPads)
- USB Drives
- CDs
- External hard-drives
- Laptops –and–
- MP3 players

For example, a court found that an employee misappropriated his employer's trade secret when, on the last day of his employment, he transferred confidential information from his work laptop to a CD that he intended to keep for his personal use. LeJeune v. Coin Acceptors, Inc., 381 Md. 288, 314 (Md. 2004).

To avoid trade secret theft by means of mobile or portable storage devices, employers should implement policies that prohibit or limit the use of external devices that can electronically introduce, store, and remove protected data and information. If storage on a

mobile or portable storage device is necessary, policies should specify that employees must obtain authorization to store information on the device.

Employers should also consider encrypting their confidential information so that any information that must be stored outside the employer's network is still protected. This is especially true where the information being stored contains confidential personal identifying information, including, among other things, employee names, addresses, bank account numbers, and social security numbers. See, e.g., First Financial Bank, N.A. v. Bauknecht, 71 F. Supp. 3d 819, 829 (C.D. Ill. 2014). In *First Financial*, the employer's policy deemed customer account information, financial data, and personal information to be confidential. Id. It also required encryption of data copied onto laptops or other storage devices. The employer trained its employees on how to remove confidential information from personal iPads. Id. The court held that these steps, along with requiring its employees to sign a confidentiality agreement, constituted reasonable efforts to protect its trade secrets. Id.

Policies restricting use of portable storage and mobile devices should also emphasize that storage on a mobile or portable device must be temporary. The device must be cleared as soon as the need for temporary storage ceases. For example, employers should consider implementing a system wherein employees must check out mobile and portable storage devices and check in the portable storage and mobile devices when the employees no longer need them. This allows the employer to control possession and dissemination of mobile and portable storage devices and to ensure devices are properly "wiped" or cleaned after the employee returns them.

Prevent Physical Removal of Confidential Information

In addition to restricting digital removal of confidential information, employers should also take steps to restrict its physical removal. Employers should adopt policies prohibiting removal of confidential information and employer records from the business premises. See, e.g., Morgan Stanley Smith Barney LLC v. O'Brien, 2013 U.S. Dist. LEXIS 159128, at **1, 7 (D. Conn. Nov. 6, 2013) (employer successfully obtained an injunction against a former employee who misappropriated trade secrets where the employment agreement prohibited employees from removing trade secrets or employer records from the business premises, in their original or copied form).

In addition, employers may implement measures such as restricted printing permissions for electronic information that is flagged as confidential, or only permit certain employees to have printer access. Restricting the physical removal of confidential information is one more precaution aimed at avoiding unauthorized dissemination.

Take Advantage of Network and Information Protection Technology

The following cybersecurity measures may also assist in preventing unauthorized entry into an employer's network and/or computers.

Firewalls

A firewall is a type of software designed to monitor and control inbound and outbound network traffic. Employers use firewalls to prevent users outside of an employer's network from getting into it and accessing confidential information. Courts have found that an employer's use of a firewall, along with other measures, constitutes reasonable efforts to keep confidential information secret. See, e.g., Hamilton-Ryker Grp., LLC v. Keymon, 2010 Tenn. App. LEXIS 55, at *15 (Tenn. Ct. App. Jan. 28, 2010) (holding an employer's use of a firewall-protected server, confidentiality agreements with employees, and limitations on employees' electronic access to documents were reasonable steps to keep information confidential).

Data Encryption Software

Encryption software is designed to alter information and files into unreadable codes that can only be deciphered by the employer's own encryption software. Encryption is an effective tool when an employee or unauthorized user removes confidential information from a company computer or network and tries to access it on a non-company computer, making it impossible for him or her to actually open and view the confidential information. Thus, encryption is useful because it prevents the individual from accessing and using confidential information.

Website Access Blocking Software and Internet Use Restrictions

An employee's access to untrustworthy websites can introduce malware to an employer's equipment and networks, which could ultimately harm confidential information stored within the equipment and networks. To assist in preventing malware from untrustworthy websites, employers may consider using software that blocks access to these websites and adopt a policy that informs employees about unacceptable Internet uses.

Cybersecurity Software

There is a wide variety of computer security software that can perform a range of security functions, from preventing the introduction of malware to monitoring and flagging suspicious activity. The following list provides some examples of objectives that cybersecurity software may achieve:

- Prevent, detect, and remove malware
- Generate pop-up messages that appear any time an employee engages in computer or network activity that poses a risk to the security of confidential information
- Monitor e-mail activity and limit the types of data or information that employees can transfer outside of the organization
- Detect and prevent unencrypted documents from being downloaded

For example, an employer successfully alleged that its misappropriated information was confidential where it demonstrated that it used a private network encryption program, secure passwords, on-screen confidentiality warnings, and bold "Confidential" boxes around confidential information. PartyLite Gifts, Inc. v. Macmillan, 2010 U.S. Dist. LEXIS 133440, at *4 (M.D. Fla. Nov. 24, 2010). In *PartyLite*, the employer's code of conduct also required employees to protect the information, and employees with authorized access had to sign confirmations of compliance each year. Id. *PartyLite* illustrates the effectiveness of using a combination of cybersecurity software and confidentiality policies when working to establish that the employer took reasonable steps to protect its trade secrets and confidential information.

Continuously Monitor and Improve Cybersecurity Measures

Employers should consistently monitor and improve their cybersecurity measures over time and as incidents arise. Employers may use monitoring efforts to demonstrate that they are taking reasonable steps to implement and improve their cybersecurity measures and protect their trade secrets, as required under state Uniform Trade Secrets Acts and the DTSA. This includes monitoring network activity, e-mail usage, and access to information and systems to identify unauthorized or suspicious activity. See, e.g., First Financial Bank, N.A., 71 F. Supp. 3d at 844 (employer took reasonable steps to protect its trade secrets where it monitored employee access to hard and electronic copies of confidential information).

Employers should retain the right in their non-disclosure/confidentiality or other employment agreements and technology and computer use policies to record, store, access, audit, delete, and review any information, including business and non-business e-mail, voicemail, instant messages, word processing documents, spreadsheets, etc. stored on their systems. Retaining these rights will allow an employer to monitor its confidential information consistently and as the need arises. See Creating Policies on Computers, Mobile Phones, and Other Electronic Devices and Computers, Mobile Phones, and Other Electronic Devices Policy.

In addition to monitoring employee usage, employers should monitor their own systems for vulnerabilities and opportunities for technology and software updates. Keeping computer and network systems up to date will help improve the chances of fending off malware or hackers. Advise employers to proactively engage data security consultants to develop, implement, and maintain data security plans.

Who Should Be Involved with Oversight of Trade Secrets within a Company?

Each time an employer creates a new product line, undertakes new initiatives, or acquires new information that constitutes a trade secret, it should consider tasking a person or group of people to consider and identify how the new development implicates cybersecurity needs. This allows the employer to maintain knowledge as to what trade secrets it has so that it can implement reasonable efforts to maintain their secrecy.

Employees who are senior, with visibility and access across the company, and who have business, legal, and technical experience may be the most qualified to determine what needs to be protected and how to best protect it. For example, the appropriate person may be the chief information officer, chief information security officer, chief legal officer, or someone in a similar position. Or, the group may be a combination of these individuals. Regular communication with the information technology department (if applicable) is also critical to ensure that others who work with company software and intranet are aware of any cybersecurity measures in place. Whether one employee is in charge of oversight or whether multiple roles work together will depend on the nature of the company.

The employer's board or a committee of the board may also have some involvement in information security, but how it interacts with others involved in information security will vary by employer.

What Are the Best Practices for Planning for (and Responding to) a Theft/Loss of Trade Secrets Due to Employee Conduct

Employers should develop a response plan in the event of theft or loss of a trade secret due to employee conduct. A trade secret theft/loss plan may include the following steps:

Step 1: Assign Incident Roles and Responsibilities

Before any trade secret theft or loss occurs, assign incident roles and responsibilities to employees who will be involved in the response process, such as information security employees, legal counsel, and managers. A team that is prepared can help ensure an efficient response.

Step 2: Institute Response Protocols

Upon learning of trade secret theft or loss, the employer should ensure a timely shut off of the employee's remote access to employer systems and e-mail, and retrieve any and all information, documents, and devices the employee may possess.

When theft or loss of a trade secret occurs, employers should contact, through legal counsel, the misappropriating employee and demand, among other things, that he or she return any stolen materials and refrain from using or disclosing the trade secret information. The employer can set forth the applicable statutes that the employee may have violated and/or may be violating in the form of a cease and desist and/or demand letter. The letter should also demand that the employee preserve all information relevant to the dispute and return any materials or devices that remain in the employee's possession. This letter serves as formal notice that the employee is in breach of his or her contractual obligations and also provides evidence that the employer has taken reasonable and prompt measures to protect its trade secrets. Even if the employee does not respond or comply, this initial contact is useful in the event a temporary restraining order or injunction is necessary, as courts are hesitant to grant *ex parte* injunctions.

The employer should also assess the damage and extent of theft or loss by retaining a forensic expert to collect and search electronically stored information. The expert may engage in forensic investigation of the employee's devices, which the employer may use as evidence of employee wrongdoing in the event the employer pursues litigation against the misappropriating employee.

For more information on potential pre-litigation tactics, including cease and desist letters and use of forensic investigators, see Pre-litigation Steps in Trade Secret Misappropriation and Breach of Restrictive Covenant Litigations.

Step 3: Determine Whether an Injunction Is Warranted

Employers should enlist legal counsel to determine whether seeking a temporary restraining order or injunction is appropriate. A request for a temporary restraining order or preliminary injunction will set forth a description of the trade secrets the employee misappropriated and emphasize that the employer will be immediately and irreparably harmed if the employee uses or discloses trade secret information. It must also show that the employer is likely to succeed on a trade secret misappropriation claim and demonstrate that the balance of hardships tips in favor of the employer. Counsel who file a motion for a temporary restraining order or preliminary injunction should be prepared to argue the motion within hours of its filing, depending on the jurisdiction in which the motion is filed. See Pre-litigation Steps in Trade Secret Misappropriation and Breach of Restrictive Covenant Litigations.

What Cybersecurity Precautions Should an Employer Take for Employees Who Resign or Are Terminated?

As part of the normal termination process, employers should implement preservation and investigation protocols for every employee who terminates his or her employment, whether voluntarily or involuntarily. These protocols should be well-established and consistent to allow the employer to move quickly, as courts may consider the speed with which an employer reacts to potential trade secret theft as a factor in a trade secret misappropriation action.

For instance, a court found that an employer took reasonable efforts to maintain the secrecy of its source code when, in addition to its cybersecurity measures—including password-protecting its computers and network, storing computer servers in a locked room, requiring all employees to use RSA security tokens, requiring programmers to work in their own locked office, limiting access to the source code, and requiring employees to agree not to share their work with others—the employer immediately terminated an employee upon learning he had copied and removed source code from the employer's premises. Geraci v. Macey, 2016 U.S. Dist. LEXIS 89240, at *5 (N.D. Ill. July 11, 2016).

The following steps are potential precautions an employer can take when an employee departs:

- Remove the former employee's network access.

- Immediately collect the former employee's corporate devices (phones, laptops, tablets, etc.). See Drafting Exit Interview and Return of Company Property Policies and Exit Interviews and Return of Company Property Policy.
- Archive the former employee's entire e-mail system, including sent and deleted items.
- Delete company software and data from the former employee's personal device(s).
- Issue a separation letter to the employee, reminding him or her of his or her post-separation obligations, including those of non-disclosure and confidentiality. See Understanding, Drafting, and Negotiating Separation Agreements on Behalf of Employers and Separation Agreement.
- Preserve documents, information, and equipment on which the former employee worked. The length of preservation will vary depending on the circumstances of the employee's departure:
    - Preserve for several months as a regular practice.
    - Preserve as long as required, if subject to a litigation hold.
    - Preserve for longer than regular practice, if the circumstances of the employee's departure are suspicious (e.g., he or she leaves abruptly, is disgruntled, etc.) and the employer foresees litigation.
- Conduct exit interviews of departing employees to identify confidential information they may possess; retrieve it, and ensure they know they cannot use it in future jobs with other employers. See Drafting Exit Interview and Return of Company Property Policies and Exit Interview Questionnaire.
- Issue a cease and desist letter to the employee if the employer discovers that the employee misappropriated trade secrets. Doing so creates a paper trail for litigation and serves as a bridge for moving for injunctive relief. For more information on cease and desist letters, see Pre-litigation Steps in Trade Secret Misappropriation and Breach of Restrictive Covenant Litigations. For annotated cease and desist letters, see Cease and Desist Letter to New Employer Regarding Post-employment Restrictions and Cease and Desist Letter to Former Employee Regarding Post-employment Restrictions.
- Arrange for and conduct a thorough forensic analysis, including copying the hard-drives and files on every device that will need to be forensically examined.

For additional information on protection of confidential information at termination, see Trade Secrets and Confidential Information Protection upon Termination Checklist.

What Issues May Arise When a Data Breach Involving Trade Secrets Occurs?

When a data breach involving trade secrets occurs, employers are faced with multiple issues, such as:

- Identifying which trade secrets were compromised
- Identifying who caused the breach –and–
- Addressing any loss of value to the business

Identifying Trade Secrets

Many types of data and information may constitute a trade secret. Even a small company can have a large number of trade secrets, such as product blueprints, financial information, customer lists, and marketing plans. Yet, many employers may not have a structured system in place to identify, value, and protect trade secrets. Therefore, the first issue an employer may face when an employee misappropriates a trade secret is that the employer has not yet identified the trade secret as a trade secret. As a result, the employer will not have determined the trade secret's value, taken steps to designate it in some manner as confidential, or otherwise protect it as a trade secret prior to the misappropriation.

Not identifying trade secrets as trade secrets may result in delayed incident response. Once a misappropriation occurs, the employer will have to spend valuable time and resources to determine whether and what trade secrets were compromised. An employer that fails to quickly respond to misappropriation weakens its argument that it took reasonable steps to protect its trade secrets. Delay may also lessen the employer's success in obtaining an injunction or temporary restraining order, as "delay in pursuing a preliminary injunction may raise questions regarding the plaintiff's claim that he or she will face irreparable harm if a preliminary injunction is not

entered." Motorola, Inc. v. DBTEL Inc., 2002 U.S. Dist. LEXIS 13240, at *19 (N.D. Ill. July 22, 2002) (quoting Ty, Inc. v. The Jones Grp., Inc., 237 F.3d 891, 903 (7th Cir. 2001)).

Trade Secret Audits

To avoid these potential consequences, the identification, categorization, and protection of trade secrets should be an ongoing practice. Employers have multiple methods available to conduct a trade secret audit as a first step toward identifying and protecting their trade secrets. Internal staff can conduct manual audits, but they may not have the requisite expertise to evaluate what constitutes a trade secret. Outside consultants can also conduct a manual audit, bringing their expertise and well-practiced methods to the table. Outside consultants may be more expensive, but they also offer some advantages. They may be more thorough given their expertise, and may also gain knowledge of the employer, its employees, and business, making them a valuable witness in the event of litigation. Computer-automated audits are another method for identifying confidential information. Computer-automated audits use software programs that extract and analyze data to identify valuable information that may constitute a trade secret, and detect events indicative of trade secret misappropriation.

Identifying Anonymous Actors

When a cyber-criminal or some other unauthorized entity causes a data breach (as opposed to an employee), identifying the perpetrator can be difficult, if not impossible. An employer may not have the opportunity to go on the offensive and file injunctive relief against someone whose identity is unknown. Employers may be left in a litigation limbo, where they cannot sue, but are left waiting to be sued by persons whose personal identifying information, for example, was compromised. Such a situation highlights why it is important for an employer to implement thorough cybersecurity measures and to monitor its network to increase the probability of identifying bad actors, whether they be employees, former employees, or third parties.

Loss of Value

In a competitive business environment, the difference between expanding a business and going out of business may turn on the employer's ability to implement effective cybersecurity measures to protect its trade secrets. Misappropriation of trade secrets can result in a loss of the business's value, as well as reputational harm, and in certain instances, can ultimately shutter a business altogether.

Loss of Business Value

Trade secrets are only valuable insofar as they are secret, giving an employer an economic advantage over its competitors. Once a misappropriation of trade secrets occurs, the employer's competitive advantage is in jeopardy. If disseminated, the trade secret may no longer have economic value to the employer.

Reputational Harm and Loss of Business

An employer that is unable to protect its trade secrets may also suffer reputational harm, as customers, investors, business partners, and the public may lose faith in the employer's ability to protect its information. Media coverage of the misappropriation is also a risk to a business's reputation. These reputational hits can ultimately lead to a loss of business.

To avoid these reputational harms, employers should quickly seek injunctive relief as soon as they learn a trade secret has been misappropriated. See, e.g., Arminius Schleifmittel GmbH v. Design Indus., Inc., 2007 U.S. Dist. LEXIS 10847, at *6 (M.D.N.C. Feb. 15, 2007) (granting preliminary injunction where misappropriation of company's trade secret could lead to loss of competitive business advantage or market share, goodwill, customers, and profitable business relationships).

What Are the Benefits of Bringing Claims under the Computer Fraud and Abuse Act?

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is a criminal statute that provides a civil cause of action for anyone whose computer system or network has been damaged or accessed by an unauthorized person. Depending on the facts of the situation and the judicial district in which an employer is located, an employer may be able to assert a claim under the CFAA against employees who steal trade secrets and/or confidential information from company computers. However, most employers will only be able to assert a CFAA claim if the employee caused a loss of at least $5,000 in value. "Loss" is defined as any reasonable cost to any victim, including the cost of responding to an offense; assessing damage; restoring data, programs, systems, and information to their condition prior to the offense; and any revenue lost, cost incurred, or other consequential damages incurred as a result of the interruption of service. 18 U.S.C. § 1030(e)(11).

Employers may, in certain instances and before certain courts, assert that the costs of litigation or forensic examinations should be considered as damages under the statute. See, e.g., AssociationVoice, Inc. v. AtHomeNet, Inc., 2011 U.S. Dist. LEXIS 1654, at *8 (D. Colo. Jan. 6, 2011) (holding that computer forensic investigator costs of investigating CFAA violations constituted a loss under the statute); but see, e.g., Cont'l Grp., Inc. v. KW Prop. Mgmt., LLC, 622 F. Supp. 2d 1357, 1371 (S.D. Fla. 2009) (holding forensic investigation did not constitute loss within the meaning of the statute).

The Ninth and Second Circuits' Strict Approaches to CFAA Claims

Some circuits, including the Ninth and Second Circuits, take a strict approach to CFAA claims and require true hacking or criminal activity to impute liability to a bad actor. This usually does not apply to employees who access confidential information by virtue of their employment. See U.S. v. Nosal, 844 F.3d 1024, 1028 (9th Cir. 2016) ("'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."). See also U.S. v. Valle, 807 F.3d 508, (2d Cir. 2015) (agreeing with the Ninth Circuit's definition of "exceeds authorized access").

The Seventh Circuit's Broader Approach to CFAA Claims

On the other hand, other circuits, including the Seventh Circuit, take a broader approach and allow employers to bring claims against employees who exceeded their "authorized access" or accessed a system without authorization (e.g., post-termination) to obtain confidential information. The Seventh Circuit has broadly construed "authorized access" to include breaches of the duty of loyalty. See, e.g., Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (finding that employee exceeded authorized access by accessing information after he had breached the duty of loyalty).

CFAA Statute of Limitations

Employers must keep in mind that they must bring CFAA claims within two years of (1) the date the unauthorized access occurred or (2) the date the employer discovered the damage or unauthorized access. 18 U.S.C. § 1030(g).

Benefits of a CFAA Claim

Pursuing a claim under the CFAA may assist an employer in several ways:

- First, bringing a claim against an employee under a criminal statute demonstrates the seriousness of his or her actions.
- Second, it serves as a deterrent for those employees and/or former employees possibly considering misappropriation.
- Third, the CFAA allows for the allegedly injured party to move for injunctive relief in an effort to quickly stop an employee from using the employer's protected information. 18 U.S.C. § 1030(g).
- Fourth, employers do not have to prove that an employee stole a trade secret. Instead, the CFAA only requires the employer to show that the employee wrongfully accessed the information. See, e.g., Fiber Syst. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1168 (5th Cir. 2006) ("Section 1030(a)(4) does require a finding that the violator obtained something of value by means of the unlawful access, but the value need not be a trade secret or even something that was stolen."). In this regard, a CFAA claim may, in certain instances, be easier for an employer to plead than a claim for trade secret misappropriation, as not all confidential information rises to the level of a trade secret.

For more information on CFAA claims, see the "Computer Fraud and Abuse Act" section of Strategies for Bringing Counterclaims or Separate Lawsuits against Plaintiff Employees — Types of Claims against Employees.