How to keep the lid on your ‘secret sauce’

Although there is no one-size-fits-all approach, Li Zhu and Christine Yun Sauer of Robins Kaplan offer a set of best practices for protecting your trade secrets

For decades, companies have turned to the patent system to protect their inventions. Patents provide broad protection by granting an effective monopoly against competitors for 20 years—a monopoly that often survives the effective shelf-life of the invention in the marketplace. The tide, however, is undoubtedly changing. Patents in key sectors such as software are becoming more difficult to obtain and protect. Many believe the patent system is under assault in light of the newly created patent office inter-partes review procedures, numerous attempts by US Congress to curtail patent enforcement, and the Supreme Court’s decision in Alice Corp v CLS Bank. Given this perceived uncertainty, many companies are turning to trade secret protection to guard their intellectual property. Should your company be following suit?

The power of trade secrets

Within the 48 states that have adopted the Uniform Trade Secrets Act (UTSA), a “trade secret” is defined as any information, including formulas, patterns, compilations, programs, devices, methods, techniques, or processes, that (i) derives independent economic value, whether actual or potential, from not being generally known to the public or people who can obtain economic value from its disclosure or use; and (ii) is protected by reasonable efforts to ensure its secrecy under the circumstances. Put simply, a trade secret is designed to protect a company’s ‘secret sauce’—information that is valuable because it is unknown to others.

Trade secret protections, under state law and the comparable federal cause of action created by the Defend Trade Secrets Act (DTSA) of 2016, provide a legal mechanism for preventing competitors from stealing or misappropriating those secrets, as well as money damages if misappropriation occurs. Such protection is especially attractive to companies that want to keep their information secret for an indefinite amount of time, or require immediate protection without the expense of patent filing and prosecution fees. In most states, an injured company can recover money damages against a defendant who receives trade secrets that the defendant “knew or had reason to know” were acquired by improper means, such as theft, espionage, or unauthorised disclosure. However, this protection is only available in situations where the owner of the trade secret takes reasonable efforts to ensure that information’s secrecy.

Best practices

Inventory and mark trade secrets: Identify what your company believes to be its trade secrets. A comprehensive inventory will usually request input from both technical advisors and attorneys. The company should then unambiguously mark documents, files and other sources that embody these trade secrets as ‘confidential’ or ‘trade secret’, both for internal recordkeeping and in case they are ever transferred to an outside vendor (such as for cloud storage or as part of a contract services agreement). Clearly identifying and segmenting such information can help prevent inadvertent disclosures, and may be necessary to trigger certain confidentiality provisions in vendor agreements.

Assess hiring procedures: Take several precautions during the hiring process to avoid liability for trade secret misappropriation or improper solicitation. First, confirm whether candidates have any confidentiality agreements or restrictive covenants with current or prior employers, and review those agreements before extending an offer (or condition the offer upon such review). Otherwise, the company may be forced to choose between a lawsuit filed by those companies or a candidate’s wrongful termination suit. Second, have candidates agree in writing not to bring, retain, use, or access any information from former employers (including through the former employer’s email, voicemail or computer systems), or solicit former co-workers. Third, notify candidates in writing that their potential hiring is not based on their knowledge or possession of any former employer’s confidential information. Last, ensure candidates sign all necessary agreements before starting work.

Assess key agreements: Ensure that every employee signs several key agreements. Non-disclosure agreements (NDAs) should instruct employees not to disclose certain information (including trade secrets) to unauthorised entities. Assignment agreements that expressly assign an employee’s ideas and inventions to the company should be written in the present tense (for example, ‘I hereby do assign’), detail the subject matter assigned, and provide an exception for inventions created using the employee’s own time and resources. Non-solicitation agreements prevent a former employee from actively soliciting current employees, and should be limited in term (one to two years) and scope (ie, applying to individuals that the former employee worked with and/or became aware of while still employed). Outside counsel can often review these agreements quickly to identify loopholes and provide valuable feedback.

Strengthen internal protections: Assess the company’s internal procedures for protecting trade secret information. This includes evaluating both physical (for example, secure rooms and access cards) and data security protections (for example, encryption, firewalls, backup and recovery), as well as other compliance standards. It is particularly important to limit access to trade secret information to those who need it and to compile the resulting access list in case misappropriation occurs.

Vendors: Due diligence means investigating vendors that may receive trade secret information and assessing their physical and virtual security practices, track record, and recent intrusion testing results, among other things. Ask the important questions: does the vendor store the data itself or employ a cloud service? Does the vendor have extensive security measures to protect

against hackers? Does it encrypt highly sensitive data? Is proprietary information segregated (siloed) from other data? How current is the vendor's back-up and recovery system? Does it have robust data deletion procedures? In short, vendors should be established, reliable, and reputable.

After selecting a reputable vendor, the company should negotiate terms of service (TOS) and service level agreements (SLAs) to better ensure the security and secrecy of company data, if possible (usually available only to larger enterprise organisations). Regardless, both parties should understand where data is being kept, who 'owns' it, how it can be used, and the notification process if breach occurs.

Customised SLAs can better align a company's expectations with those of the vendor by providing objective ways to evaluate the vendor's performance, and audit rights ensure that the vendor is complying with advertised security policies.

Use exit interviews: Often ignored, exit interviews can help address potential issues so that misappropriation never occurs.

Every departing employee should have an exit interview that: (i) identifies the new employer, position, duties and responsibilities, if applicable; (ii) details the employee's access to company trade secrets during the course of employment; (iii) confirms the employee's return of company property, especially computer devices and stored media; (iv) furnishes the employee with a copy of his or her signed agreements and requests that the employee provide them to any new employer; (v) requests that the employee certify in writing that he or she acknowledges any continuing obligations under those agreements; and (vi) allows the employee to ask questions. Information gleaned during the exit interview (or from the employee's refusal to do so) can also help the company assess any risk of misappropriation and determine whether further steps are necessary.

Assess exit procedures: Several procedures should occur following any employee's departure. These include: (i) disabling the employee's access to company facilities and data networks; (ii) inspecting the employee's office and files to ensure company materials have not been compromised; (iii) assessing the employee's recent email, phone, and computer activity, and flagging any suspicious communications, downloads, or print jobs; (iv) engaging a professional who can sequester the employee's electronic devices and email communications in case forensic analysis is necessary; (v) reviewing expense reports and contacting any customers the employee was servicing; and (vi) interviewing co-workers to help assess the departing employee's intentions and flag any suspicious activities. These steps can help the company assess any risk that the employee left with sensitive information or with customers.

Establish a response team: When an unauthorised disclosure of company trade secrets occurs, your company's response team should act immediately to limit the exposure.

The team should typically include in-house and outside counsel, members of the information technology department, and include the chief information security officer (CISO) or the CISO's direct report.

The team is responsible for investigating the nature and extent of the disclosure, identifying responsible parties, and implementing remedial measures. It may also be necessary to prepare for anticipated litigation (ie, securing a chain of custody for certain items) to enforce the company's rights. For example, under the California Uniform Trade Secret Act (CUTSA), "[a]ctual or threatened misappropriation may be enjoined". Therefore, the owner of a trade secret can request help from a court in certain situations to restrict a former employee's actions or else receive compensation.

Conduct regular training: Corporate policies are only as effective as they are memorable. Regular training sessions are an important reminder of your company's expectations, especially regarding common issues such as social media. Outside counsel can be a valuable resource for training employees about important and developing legal issues.

While these best practices provide a starting point for protecting trade secrets, there is no one-size-fits-all approach. Rather, each company's strategy should be tailored to its own needs. Accordingly, companies should consult the experts. **IPPro**

Li Zhu
Associate
Robins Kaplan

Christine Yun Sauer
Associate
Robins Kaplan