Protecting Proprietary Information In Employee Departures

Sean Tuttle

Partner

stuttle@stoneturn.com

Patricia Smaldone

VP of Human Resources

psmaldone@stoneturn.com

While technology and people are often seen as key elements of a company's success, it is often not immediately apparent that there is a critical intersection between the Information Technology ("IT") and the Human Resources ("HR") functions. As companies continue to gather and retain more and more data and as employees come and go, an emphasis on protecting proprietary and confidential information is required. However, waiting until the exit interview to ensure that proper measures are in place often leaves the company open to serious risks.

Here are some ways to ensure that confidential information does not leave your organization along with departing employees.

You're Hired!

Regardless of the industry or type of organization, new employees will most likely require access to vital competitive and confidential information to do their jobs. While necessary for that employee to be productive, you can protect the company and its confidential information with the following measures.

Only provide access to confidential information to employees who need it.

In the onboarding process, it is important for HR and information technology to work together to ensure that an employee is afforded only the appropriate levels of access to various types of information on a systemic basis. For example, a new marketing employee is unlikely to require access to sensitive legal or financial information. It is best to limit access to highly sensitive information to those employees whose roles require it.

StoneTurn

Establish confidentiality polices and clearly communicate them.

Working with legal, HR should establish confidentiality guidelines for the organization. When new employees join, HR should also provide a thorough overview of the policy, as well as how the guidelines relate to the use of electronic devices. All employees should acknowledge receipt of these policies.

Bring Your Own Device

Confidential information has become accessible by all sorts of personal devices, including tablets and smartphones. This access creates opportunities for accidental or deliberate misuse of data. The policies should make clear from the beginning whether and how employees are allowed to access company e-mail and other records from personal devices, and support those policies with regular updates and system-level technology controls.

Set expectations on the types of information new employees are permitted to bring from former employers.

To protect the organization, new employees should not, and likely cannot, bring confidential information from their former employers, such as manuals, marketing materials or business contact records. This should be clearly stated and agreed in all onboarding materials, including the offer letter. This will reduce the risk of future allegations related to theft of information. It also clearly sets an expectation of ethical behavior at the firm in the onboarding process.

Working It

Over the course of the employee's tenure with the organization, it is advisable to consider potential issues that could occur in a departure, even while off-boarding is not an imminent consideration. The following serve as examples.

Continue to train employees on confidentiality policies and issue periodic reminders.

Provide consistent awareness to all employees on the importance of protecting confidential and proprietary information; frequent communications on the topic may deter employees from engaging in nefarious activities. Consider annual representations and acknowledgements to reinforce the policies.

Flag and address inappropriate behavior.

It is important for HR to have an understanding of the networking or computer monitoring tools that may be implemented and administered by IT. These tools typically have reporting options to detect inappropriate behavior related to internet usage, network share activity and file activity (e.g., deleting or copying files to an external hard drive or the cloud) For example, IT can periodically generate a report of the top five most active employees to assist HR in getting ahead of any potential issues down the road. It is always easier to prevent inappropriate actions than work to remedy issues later.

Moving On

Immediately upon an employee's departure, IT should revoke access to all systems, e-mail, remote access, mobile devices and cloud accounts, as well as physical keycard access. There are a few steps HR and IT should jointly undertake to protect the company from potential security risks.

Untangle "the spider web" of information during an employee's tenure.

Confidential company information can be stored in a growing number of places, including thumb drives, external hard drives, personal e-mail accounts, mobile devices, home computers and cloud-based repositories, among others. When off-boarding an employee, HR, working in conjunction with IT, should keep in mind the number of different locations company

information can be stored, depending upon the employee's role, the company's policy and the employee's perceived intentions, and act accordingly.

Take appropriate steps to preserve information.

Ask IT to extract and quarantine the employee's mailbox from the e-mail server for preservation purposes. The former employee's e-mail usage is often the tip of the iceberg if and when questions emerge surrounding potential theft or misuse of confidential or intellectual property.

Additionally, take possession of the outgoing employee's laptop or work station, and do not immediately repurpose the device to a new employee. In the event inquiries arise around the former employee's actions, you will need access to the computer in its original state.

Depending on the former employee's role at the company and the nature of separation, a forensic image to preserve the computer for safekeeping should be considered as a standard procedure. This creates both the preservation of the information on the device and a deterrent control. This is particularly important if the employee is joining a competitor.

Advice from counsel should be sought in the case of concerns about confidential information that might be stored on the personal device of the departing employee; again, strong and enforced policies and systemic controls can reduce the risk of such an issue.

By managing confidential information throughout an employee's tenure and clearly outlining firm policies in the onboarding process, organizations can mitigate the risk of proprietary information leaving with employees. It is also key to establish proper preventative measures to preserve employees' data upon termination, which can help protect the company in future disputes.

About the Authors

Sean Tuttle, a Partner with StoneTurn in Boston, leads the firm's Forensic Technology practice.

Patricia Smaldone, Vice President of Human Resources with StoneTurn in Boston, leads the firm's human resources function.

This article was initially published in **Law 360 in February 2017**