Why Your Company Should Be Using Email Enterprise Vaults, Anti-Deletion Programming and Key Stroke Surveillance Software in the Face of Growing Cyber Threats and Trade Secrets Theft

Insights
4.03.18

Twenty-five years ago most companies' greatest fear of espionage was employee theft at the photocopy machine at 2 in the morning. The company playbook could not be forwarded in an email or put on a thumb drive in a matter of moments and removed from company premises with no one noticing ready to be delivered by a disgruntled employee into the hands of a competitor. Twenty-five years ago companies did not have electronic document retention and production obligations any time that the company is on offense or defense in any litigation of any kind. In the last twenty-five years as technology has carried us into the digital information age so too have the tools and opportunities for cyber theft grown exponentially. Business competitors from here and abroad, in an effort to be first to market or to achieve greater market share, have benefited from defecting employees carrying the playbook with them electronically so they can hit the ground running in their new competitive enterprise all because most companies do not take advantage of low or no cost cyber theft prevention tools that every company should have as part of their IT infrastructure.

Trade secret theft by employees most commonly happens in one of three ways: 1. Employees email trade secrets from their company email to their personal email address and then delete their sent email immediately after sending the email and before most email platforms (that just perform daily back-ups of the email server) will have a record of the email being sent; 2. Employees plug a thumb drive or other external memory storage device into their company-owned computer and download the company's trade secret information onto the external memory storage device; 3. Employees connect to an internet based cloud storage service such as Google Drive and upload company trade secret information to a cloud storage account all without leaving their desk.

Given these readily available and easy to use means for employees to steal a company's trade secrets, it is critical that companies deploy basic information preservation and tracking technology to deter such theft and, in the event that theft occurs, to be able to have recorded all of the tracking information that will identify who, how and when a company's information was stolen.

Email Enterprise Vaults are actually a feature that exists on most hardware based network and email servers and can be selected as an *a la carte* item with most cloud based server subscriptions. These enterprise vaults make an automatic non-alterable non-deletable copy of every email sent or received as soon as the email is sent or received. This prevents employees from hiding the evidence

received as soon as the email is sent or received. This prevents employees from hiding the evidence of their emailing company trade secrets to themselves or a company's competitors. In the event of litigation, companies who use enterprise vaults don't have to worry about receiving litigation preservation letters since the evidence is automatically preserved and the company cannot be accused of deleting or hiding emails.

Anti-Deletion Programming is a setting that can be placed on most servers at little or no cost. This programming prevents employees from permanently deleting documents created or saved on the company network. Employees other than the CEO, Director of IT and potentially in-house counsel and the head of HR are typically the only individuals that are made aware of the existence of anti-deletion programming. They are given a secret code that only they know that, when used, automatically restores anything that had been deleted within a stated time frame (e.g. 60-90 days). A report is also automatically generated that tells these senior executives who deleted the trade secret information and when they deleted such information. Given that the law says that if you can prove destruction of trade secret information a court will equate that to misappropriation of that trade secret information, the use of anti-deletion programming is a critical tool to prevent loss of critical trade secret information and detection of the identity of the thieves engaging in such misconduct.

Key Stroke Surveillance Software is relatively inexpensive software that is incredibly valuable as an anti-theft tool. This software tracks every key stroke of every user on the network. It will detect if a user is trying to improperly download, copy, print or delete information that these users are not authorized to use in that manner and it will send an automatic warning to key senior executive personnel if an employee is accessing information the employee should not be accessing or doing something with that information that the employee is not authorized to do. Prior to a departing employee's exit interview, companies can run an activity report to make sure that the employee has not tried to steal company trade secrets prior to their departure. This software will also provide forensic evidence of theft that will be invaluable in court to prove the employee's misconduct.

In an age of high digital mobility in which a company's most valuable competitive asset is often their digital playbook data, these tools are a must to protect a company's most valuable trade secret information.

Related People

Robert Yonowitz
Partner
949.798.2113
Email