5 Tips to Help Mitigate Insider Theft

It starts with defining the line between personal and corporate information

By Julian Ackert / iDiscovery Solutions

Information is an extraordinarily prized corporate asset. In today's digital age, that information is stored electronically. For example, software companies store their highly valuable intellectual property in code repositories. Healthcare companies store personal medical records in an electronic medical record system. Sales departments within companies store sensitive trade secrets, such as client lists and pricing information, on servers and in customer relationship management systems. Electronic storage of this data does have its benefits, including backups and on-demand availability, but there are drawbacks as well. One of the main challenges for a company can be the balance between legitimate availability of this information and protection from theft.

To address this challenge, companies need to examine why this information is typically stolen. First, and most obviously, this information is highly valuable. Rogue employees can steal the information and sell it on the black market, or take it to start a competing business. Second, employees may consider the work product they created to be their own. For example, a programmer's unique algorithm for a particular function could be considered his or her own code. Or a sales representative's client list could be his or her client list. Third, employees may take proprietary information accidentally. For example, a departing employee may take an email archive file because it contains personal pictures attached to emails, but sensitive and secret corporate information may be intermixed in the same archive.

Here are five tips companies should adopt to help mitigate insider theft.

1. Define clear lines between personal and corporate information.

Not surprisingly, starting at the beginning is key to addressing some of the examples discussed above. While employment agreements will often have terms and conditions to address this, that language is sometimes lost on the employee. Taking the extra step of discussing personal, as opposed to corporate, information during the initial on-boarding process can help keep this top of mind.

This can be a bit challenging for multinational corporations, as personal information is legally defined differently across the globe. Additional complications arise when bring your own device (BYOD) protocols are implemented, as the storage medium for personal and corporate information becomes one and the same. However, setting employee expectations as they start employment, and providing periodic reminders to them, is a key component of the process.

2. Centralize the storage of sensitive information.

Employees in today's connected world need to be able to access information and work from multiple locations using multiple devices. To facilitate this, a hub-and-spoke model of information flow is often leveraged to allow the centralized server, or hub, to feed information to each of the spokes (laptops, cell phones, tablets, etc.). While centralizing proprietary information won't completely mitigate risk, a centralized server can help secure proprietary information. For example, sales data can be stored in a centralized system, with controlled levels of access to that data. Centralized storage locations can also be configured to provide very specific warnings and notifications of electronic information access. By alerting corporate security when there is unauthorized access to a file, or notifying a supervisor when an employee who has turned in his or her notice is now accessing specific pricing information, theft and breach activities can be mitigated.

3. Lock down and protect devices that access sensitive information.

A company can spend a lot of time and resources centralizing and securing their most sensitive information. Attention should also be given to the device end points that access that centralized information, such as laptops and smartphones. Specifically, the data footprint of the sensitive information on these devices should be considered. Does the device store a replica copy of the sensitive information? Is that replica copy needed on the device, or can it be configured as temporal storage? If the replica copy is necessary, is it encrypted so that a breach of the device would require a second level of authorization for access? By taking into consideration how the sensitive information is accessed by and replicated to the device, a company can improve security and control.

> ***Corporations should also consider the business needs of their employees when implementing policies.***

Devices can also be used as a transfer mechanism. For example, employees can copy proprietary information to USB drives connected to laptops. Or, alternatively, they can upload sensitive trade secrets to a cloud-based file-sharing application, like Google Drive or Dropbox. Implementing technical policies and controls around how devices are used to transfer information can better protect the most sensitive information.

Corporations should also consider the business needs of their employees when implementing these policies. For example, the complete shutdown of USB ports to prevent external drives from being connected may hamper employees' ability to do their jobs. An alternative strategy could be configuring USB ports to be read-only, which would prevent those drives from being used to copy information.

4. Ensure information is available for post-breach investigation.

In the event of a breach or theft of trade secrets, make sure that the logs, events and activity history are available for downstream investigation and analysis. Even when companies set up extremely strong safeguards on sensitive information, a breach can happen. If it does, the appropriate level of logging and activity history should be available to aid in the investigation. Because the duration and type of these logs will vary from system to system, corporations should engage with the breach response team proactively and understand what information is needed for a thorough investigation. Additionally, confirm that internal resources understand the protocols and workflows to be applied to devices and systems once a breach is identified. Shutting down or unplugging a computer belonging to a rogue employee before the incident response team has had a chance to preserve the device's memory may limit the type of historical information available for analysis.

5. Consider other sources that record employee activity.

When a breach or theft of information occurs, attention is often focused on the system breached and the employee end-point devices. However, there are other data sources that should also be considered. Are there badge swipe systems and digital recordings that can be analyzed to identify the rogue employees or bad actors? Are there GPS tracking systems in place that can help pinpoint locations of employees? Can financial systems, such as expense report tracking, be analyzed to identify patterns or anomalies? Corporations are in possession of numerous data sources storing employee activity history, and temporal analysis of this data in a layered fashion can dramatically change the results of an investigation.

There are also new technologies coming to market that proactively analyze corporate data to predict employee behavior. For example, is there an uptick in use of personal email on corporate devices? Has the tone or inflection of communications from a particular employee changed? Are the badge entry swipes and time entry tracking systems showing a difference in a particular employee's behavior? A proactive analysis of one data source may not have much predictive value, but analyzing multiple data sources proactively can paint a completely different predictive picture.

Final Thoughts

There is no magic bullet or one-size-fits-all solution, as sensitive trade secret information and employee work habits vary from corporation to corporation. While insider theft and data breaches can be very difficult to completely prevent, developing a foundation that accounts for both proactive measures and reactive analysis can help mitigate risks associated with the loss and exposure of sensitive information.

Julian Ackert, *a managing director at iDiscovery Solutions in Washington, D.C., has over 15 years of consulting and project management experience in the technology and litigation industries. He has extensive experience with forensic data collection, computer forensic analysis, and creating and implementing preservation and collection strategies. He often works with large multinational corporations to establish and develop methodologies and best practices for litigation preparedness. He can be reached at jackert@idiscoverysolutions.com.*