Consilio / ADVANCED LEARNING INSTITUTE

Consilio Institute: Practice Guide

KEEPING CONTROL OF CRITICAL DATA WHEN KEY EMPLOYEES DEPART

Consilio Institute: Practice Guide

KEEPING CONTROL OF CRITICAL DATA WHEN KEY EMPLOYEES DEPART

TABLE OF CONTENTS

KEEPING CONTROL OF CRITICAL DATA WHEN KEY EMPLOYEES DEPART

Losing a key employee is never easy. They often take with them institutional knowledge, important relationships, and critical skill sets. All this is enough of a challenge, but if they also take confidential information with them, it becomes an even more pressing data security challenge. Organizations today rely heavily upon electronically stored information (ESI) – and when employees leave, there's always a risk that they'll take some of that ESI with them when they go – either inadvertently or on purpose.

Because this can represent significant risks to organizations in terms of data security – representing risks from data privacy and security to intellectual property and competitive positioning – it's important for legal and compliance teams to both identify potential risks associated with departing employees and implement policies and procedures to safeguard valuable information.

Modern Work Practices

As companies increasingly embrace new technologies and adopt modern business practices – such as Slack, OneDrive, SharePoint, Microsoft Teams, and so forth, information is duplicated, replicated, and made more and more accessible to a broader range of employees via many devices, from desktop to mobile to cloud.

With the rise of bring your own device (BYOD) policies it's not unusual for staff to use a mix of company laptops, personal smart phones, and any number of handheld devices to access email, voicemail, documents, and data, and employees often have remote access to company servers.

These new tools and methods have greatly increased productivity and reduced friction in employees' lives. However, this new way of working can considerably increase the risk of employees walking away – even inadvertently – with commercially sensitive data. Without proper procedures in place, it is remarkably simple for departing (or current) staff to access and remove critical company data without immediate detection. Multiple devices – both personal and business – make this even more difficult. It can be much harder to prove that they've accessed or copied confidential information, making it that much harder for organizations to take remedial, disciplinary, or legal action.

Slack. OneDrive. Microsoft Teams. SharePoint.

As companies increasingly embrace new technologies, information is duplicated, replicated, and made more and more accessible to a broader range of employees via many devices, from desktop to mobile to cloud.

Prevention Is Better than Cure

It may seem paranoid, but securing data when employees leave – even amicably – is one of the best things an organization can do to protect its data. The stakes are high. Many organizations' greatest assets are their employees themselves and the knowledge they carry, both functional and institutional. And, most employees have access to a veritable mountain of competitive information, company assets that exiting staff could be tempted to remove prior to moving on to start their own businesses or work for competitors.

This information could include client lists and contact information, proprietary pricing information, strategic plans, or proprietary product roadmaps, all of which are assets no company wants to share with its competitors. Yet, because of the ease of storing, transferring, and finding this information, it is now more accessible than ever to a wide circle of employees and future ex-employees. To reduce the risk of misuse, savvy organizations must adopt a strategic approach to safeguarding confidential information.

Reducing Exiting Employee Data Theft: Top Five Tips

1. Assess the risks: The old adage that "you can't manage what you can't measure" continues to ring true. No company can evaluate risk if it doesn't fully understand the location and use cases for the tools and technology its frontline staff leverages. Ensure that you understand:

- What the tools and technology can do
- How much information they can retain
- How and where this information is stored
- Who has access to what categories of information – and why
- How the information can be transferred to other devices
- What safeguards are:
  - Currently in place
  - Available but not being fully or properly utilized

2. Collaborate with the internal IT team and with external providers: Your IT and compliance teams will have much of the information required to make this assessment. Particularly savvy IT organizations may even have an up-todate and well-maintained data map listing company asset assignments, information storage structures, role-based access controls, and more. Sometimes, an external specialist can be helpful to fully evaluate the information landscape and plan and execute the implementation of a security strategy.

3. Devise a policy: After completing a thorough risk assessment, you'll need to formulate and distribute to all staff a clearly-worded company policy on the use of technology, information, and tools. As a best practice, these policies should include, at a minimum:

- A list of the technology currently available to staff, setting out which employee categories are authorized to use which tools, and detailing those employees empowered to authorize upgrades/modifications to companyowned devices
- A list of the types of instances in which transferring company or confidential information from organizational servers and portable devices to personal/thirdparty devices is permitted and listing chain-of-command for approving such transactions
- Details about the company's policy on appropriate use of confidential information and outlines of what actions employees may be subject to should they violate that policy – up to and including disciplinary action, termination, and civil or criminal prosecution
- Explanation of the company's comprehensive monitoring strategy as a deterrent against wrongdoing
- Access restrictions around certain activities, such as blocking cloud-based email like Gmail or cloud-based storage like Dropbox

4. Administer the policy: A policy is nothing if not well-enforced. If you're serious about securing your confidential corporate information, you'll want to appoint a team whose task it will be to:

- Administer the policy
- Monitor abuse
- Keep abreast of technological developments and their implications for the policy
- Implement changes as technology evolves

5. Defend against IP and data theft: Your organization may have implemented many protective measures to minimize the risk of data loss upon the departure of a valued employee, but there is no way to ensure 100% success. As such, it is critical for organizations of all sizes to implement a consistent and thorough departing employee program to investigate departing employees and defend against theft of your data through:

- **Preservation:** First and foremost, preserve and collect the departing employee's data assets using forensically sound methodologies to protect the state of the data. This can be done on the employee's phone, computer, flash drives, and on other ESI sources.
- **Investigation:** There are common means for an employee to exfiltrate data from their employer's data assets prior to their departure. An effective departing employee program should evaluate artifacts to unmask these exit points:
  - **Email Analysis:** The most common method for data exfiltration is through email. An employee may email files to their new employer or to their personal email account, then cover their tracks by deleting those email communications. An effective email analysis should thoroughly review both deleted and non-deleted emails.
  - **USB Analysis:** When an employee steals large amounts of data, they will often use an external flash or hard drive. A USB Analysis will reveal USB mass storage devices and often uncover mass exfiltration of corporate IP.
  - **Deletion Analysis:** Departing employees may destroy data upon their departure by deleting files and folders. Through the use of specialized digital forensic software, these folders and files may be recovered and returned to their rightful owners.
  - **File Activity Reports:** The best way to learn what the departing employee was doing is to evaluate file activity through LNK File, JumpList and other hidden system databases located on their recovered computer or mobile device. This analysis can reveal access to sensitive IP and show what the departing employee was up to during their final days of employment.
  - **Internet History Analysis:** A thorough analysis of a departing employee's internet usage may reveal evidence of spoliation, data tampering, or even nefarious behavior. Internet history might show Google searches such as "how to copy contacts from Outlook" or "how to permanently delete a file." The internet is the lifeblood of our day-to-day computer usage and can reveal a lot about what a

departing employee was doing on their computer.

- **Anti-Forensic Analysis:** When a departing employee has stolen sensitive IP they may often try to cover their tracks by using anti-forensic software like BleachBit or CCleaner. Although these tools may be effective at covering the departing employee's tracks, they always leave traces behind which can be easily uncovered and used to show a departing employee's intent.

Post-mortem: Getting Smart after the Event

The best-laid security and policy plans still cannot guarantee 100% compliance, and ne'er-do-well departing employees may still succeed in removing confidential information. If a breach is discovered (and it may be a matter of "when," rather than "if"), companies with well-laid out policies may resort to legal action to stop the use and dissemination of confidential or company-owned information.

> "The most common method for **data exfiltration** is through **email**...then [employees] cover their tracks by deleting those **communications**."

However, it can be difficult to take action against former employees in cases where the company has failed to retain the exiting employee's data. Crucial information is often contained on ex-employee's desktops, laptops, or smartphones, as well as in chat logs and on email servers or archive tapes. Without careful, professional preservation and management of the data, it will not remain useful for long. Data is volatile, especially metadata (the invisible record of who has created, amended, and read a document – metadata is data about data), and can be damaged by being copied or backed up in the wrong way, permanently eroding its evidentiary value. In particular, it is quite usual for the equipment of ex-employees to be reallocated quickly to another member of staff, which means that the former employee's data is overwritten or amended, while email back-up tapes – especially in smaller companies - may be overwritten frequently.

Without a comprehensive set of policies and procedures for handling exiting employees, it may not become apparent that confidential data has been stolen or misused until days, weeks, or months after an employee has left. If the data the employee stole is wiped, reassigned, or otherwise lost due to incorrect or incomplete data and equipment policies, the evidence may be lost, making it much harder to even assess the extent of the damage, let alone seek compensation, remedial action, or pursue litigation.

Conclusion

Modern tools and technology have both made our lives easier and far more complex. No one would wish for data to be harder to transfer or share. Sensitive data, however, must be protected from potential bad actors.

With careful planning and vigilantly enforced policies and procedures, organizations can manage the risks, ensure that their confidential information is protected, and safeguard their competitive advantages when key employees depart.