WHITE PAPER

Best Practices for Protecting Your Data When Employees Leave Your Company

An Osterman Research White Paper

Published December 2016

Sponsored by

ARCHIVE360
POINT. CLICK. MIGRATE. STORE.

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

When employees leave a company, whether voluntarily or involuntarily, it is quite common for them to take sensitive and confidential data with them. This paper examines this problem in detail and provides solutions for employers to mitigate the risks. For example:

- A survey published by Biscom in late 2015 found that 87 percent of employees who leave a job take with them data that they created in that job, and 28 percent take data that others had created. Among the majority who took company data with them, 88 percent took corporate presentations and/or strategy documents, 31 percent took customer lists, and 25 percent took intellectual property[i].

- A survey of 1,000 employees in the United States and Europe found that one in five had uploaded sensitive and confidential corporate data to an external cloud service specifically for the purpose of sharing it with others[ii].

- As just one example of data theft by departing employees, in September 2016 the US Office of the Comptroller of the Currency (OCC) detected the November 2015 theft of more than 10,000 records by a retiring employee that may have exposed personal information about OCC employees[iii].

KEY TAKEAWAYS

Here are some of the important takeaways presented in this paper:

- Employee turnover is a fact of life: the typical organization in the United States, for example, can expect that 24 percent of its employees will leave each year, although some companies in the Fortune 500 experience much higher turnover[iv].

- Employees who leave their employers, regardless of the reason for their departure, often take with them sensitive and confidential information, such as intellectual property or trade secrets, that belongs solely to their employer.

- The theft of this information can damage a company in a variety of ways, including putting them at risk of a regulatory violation, forcing them to take legal action against former employees, harming their competitive position, and negatively impacting their revenue.

- To reduce the risk of employees taking information with them when they leave, employers should establish detailed and thorough policies and procedures focused on ensuring visibility into employee practices, limiting employee access to data, requiring encryption of sensitive data, managing devices properly, ensuring that data is backed up and archived properly, requiring the use of enterprise apps (since these apps and any associated offline content can be remotely wiped, even on personally managed devices), and ensuring that IT has access to all corporate data to which it *should* have access (some confidential data, such as HR data, should not be available to IT in all cases.)

- To support these policies and procedures, organizations should evaluate and deploy various technology solutions. Technologies that should be considered, but not all of which need to be deployed, include content archiving, backup and recovery, file sharing and collaboration, encryption, mobile device management, employee activity monitoring, data loss prevention, logging and reporting, virtual desktops and other solutions that will minimize the possibility of employees misappropriating corporate data upon their departure.

ABOUT THIS WHITE PAPER

In support of this white paper, Osterman Research conducted an in-depth survey of 187 IT and/or HR decision makers and influencers in organizations of various sizes,

When employees leave a company, whether voluntarily or involuntarily, it is quite common for them to take sensitive and confidential data with them.

primarily in North America. Some of the results of that survey are included in this white paper, but the full survey results will be published in a separate survey report.

This white paper and survey were sponsored by Archive360. Information about the company is included at the end of this paper.

EMPLOYEES LEAVE COMPANIES

The United States Bureau of Labor Statistics reports that, as of January 2016, the median tenure of employment for US-based employees was 4.2 years, slightly shorter than the 4.6 years reported in January 2014[v]. This means that the typical organization can expect an annual turnover of about 24 percent of its workforce each year. However, Millennials (those aged 18 to 34 years) change jobs about every two years, and so the problem of turnover is likely to become worse as Millennials become a larger proportion of the workforce.

Moreover, while most employees leave organizations voluntarily, there are hundreds of thousands of involuntarily terminations each year, primarily reductions in force. For example, in 2016 alone the US tech industry is expected to lay off more than 260,000 employees[vi], and the US oil industry laid off more than 350,000 employees[vii], to name just two of the many industries in which layoffs have been a relatively common occurrence.

EMPLOYEES LEAVE COMPANIES WITH CORPORATE DATA

While employee turnover and terminations bring with them a variety of corporate, financial and logistical problems, they also create a wide range of data protection and data management problems, as well. For example, respondents to the survey conducted for this white paper reported a variety of problems related to employee turnover and terminations, as shown in Figure 1.

Employee turnover and terminations bring with them…a wide range of data protection and data manage-ment problems.

Figure 1
Problems Related to Data Protection
Percentage of Respondents Indicating Significant or Major Problems

Source: Osterman Research, Inc.

While there are generalized problems associated with loss of corporate expertise when employees leave, many of these problems are related to employees actually taking data with them when they depart, or leaving it in locations that are unknown or inaccessible to corporate data managers.

Many employees leave their employers with a wide variety of data types that can include confidential or sensitive financial data, information on customers and key accounts, various types of intellectual property, price lists, marketing plans, sales data, their database of contacts, company directories, competitive intelligence, product plans and other information that belongs to their employer.

WHY DO THEY TAKE DATA WITH THEM?

Employees who leave with corporate data when their employment has ended do so for one (or more) of three reasons:

- **They do so inadvertently**
  In an era of Bring Your Own (BYO) devices, cloud applications, cloud storage, mobile apps and other elements of "shadow IT", departing employees can often leave with substantial amounts of corporate data and not even realize or remember that they still possess it. Moreover, because a large and growing proportion of employees work at least some of the time from home, if only after normal work hours, they often maintain a rich source of corporate data on their personal desktop and laptop computers, USB sticks, personally managed file sync and share tools like Dropbox, and in other locations.

- **They don't feel it's wrong**
  Some employees will knowingly leave with corporate data upon their termination because they don't feel it's wrong to take it with them, or that it will not harm the company. For example, an employee who has worked to foster key client relationships, created valuable intellectual property, or is leaving a financially troubled company that may soon be going out of business may feel justified in taking corporate data with them, often because they feel the data belongs to them. The problem is exacerbated by corporate data protection policies that are not enforced or by the lack of security or monitoring technologies designed to protect against data exfiltration.

- **They do so with malicious intent**
  Some employees will take corporate data with them upon their departure with malicious intent. Some employees might be angry with company management because they were laid off or otherwise terminated involuntarily, they might have been passed over for a promotion, they may have a personal dispute with their manager, or they might want to gain an advantage in their new job by having sensitive or confidential information from their former employer. While employees who take and/or destroy data maliciously may represent only a small proportion of total data loss in an organization, the damage they do can be significant.

Departing employees can often leave with substantial amounts of corporate data and not even realize or remember that they still possess it.

SIGNS OF UNUSUAL EMPLOYEE BEHAVIOR

When employees are planning to steal corporate data or are in the process of doing so, there are often one or more signs to which management should be sensitive:

- Employees will copy information to the cloud, USB drives, personal devices, personal email accounts, personal file sync and share accounts, other cloud storage systems and to other venues. While this is a common occurrence in the era of BYO and is often performed by employees who are simply doing their job, a spike in any of these activities might be a sign that an employee is about to leave and is exfiltrating data in advance of his or her departure.

- A significant number of documents deleted from an employee's desktop or laptop computers, corporate file shares and other data repositories.

- Sudden spikes or drops in email activity.
- Unusually timed employee access to corporate accounts or facilities, such as a CRM system or financial account that is accessed at odd hours or differently than the employee's normal pattern of accessing this information.
- Emails or other communications sent or received between an employee and competing organizations.

THE CONSEQUENCES OF EMPLOYEES LEAVING WITHOUT APPROPRIATE PROCESSES IN PLACE

Data exfiltration on the part of departing employees can create a variety of problems, ranging from the simply annoying to those that could potentially put a company out of business. Compounding the problem is that more than one in five of the organizations we surveyed for this white paper does not have a way of retrieving data that was under the control of employees when those employees leave.

LOSS OF INTELLECTUAL PROPERTY

Most businesses have trade secrets, designs, patents, customer lists or other confidential information that constitute a valuable store of intellectual property upon which they depend to run their business. If this data is taken by a departing employee, it can cause significant harm to a company's finances, revenue prospects or reputation, not to mention the sometimes significant cost of engaging in litigation. Here are a few examples to consider:

- While he was an employee, an IT technician at Expedia's Hotwire.com division hacked into company executives' devices and used the inside information he obtained to generate more than $330,000 in stock option trades. Although the employee left Expedia in 2015, he continued to use a company laptop that he had not returned upon his departure, accessing devices and email accounts used by company executives until he was caught in 2016[viii].
- A former manager at the industrial division of Ferguson Enterprises, a plumbing wholesaler with more than 39,000 employees operating in 25 countries and listed on the London Stock Exchange, is alleged to have copied sensitive information, including contact information for customers, onto a USB drive and via his personal Dropbox account for the purpose of setting up a competing facility[ix].
- A software development manager at BlueScope learned she was to be terminated and immediately began downloading a large number of BlueScope's trade secrets. The company believed the data to be so sensitive that it initiated an emergency legal action in the Federal Court of Australia, as well as in Singapore, to prevent competitors from accessing the data[x].
- Atlantic Marine Construction Company initiated legal action against a former vice president of the company, alleging that he stole trade secrets from the company *after* his termination. The suit alleges that the former employee had installed Google Chrome Remote Desktop without authorization while he was employed by the company, and then accessed the company's network at least 16 times after he left for the purpose of exfiltrating various types of confidential information[xi].
- An employee of Leica Geosystems in Australia downloaded approximately 190,000 files containing sensitive and confidential information the day before he submitted his resignation. On his last day with the company, he deleted roughly 54,000 of those files, but downloaded an additional 190,000 files during a five-hour period. Leica sued the employee in the Australian federal courts, the result

More than one in five of the organizations we surveyed…does not have a way of retrieving data that was under the control of employees when those employees leave.

of which was a fine of AUD$50,000 levied against the employee[xii].

LAWSUITS AND OTHER LITIGATION

Loss of intellectual property and other examples of data exfiltration by former employees can lead to lawsuits and other litigation, both on the part of employers who are suing ex-employees, as well as countersuits from former employees.

LOSS OF REGULATED DATA OR DATA SUBJECT TO LEGAL HOLD

An employee who exfiltrates or deletes data upon his or her termination can cause serious harm by placing his or her former employer out of compliance with a regulatory obligation by breaching the data, or preventing that company from complying with its legal obligations, such as data that is subject to a litigation hold or court-ordered eDiscovery. This data might include Protected Health Information (PHI), Personally Identifiable Information (PII) or data that is subject to Payment Card Industry Data Security Standard (PCI DSS) requirements. The issue here is that misappropriated data can not only put an organization at risk for its potential to be exposed, but also data that an employee may have deleted or wiped from their device upon termination that is relevant to an on-going investigation or litigation, such as a patent suit.

LOSS OF COMPETITIVE ADVANTAGE

The exfiltration of data by departing employees, particularly those in key positions in sales, marketing, senior management, etc., can result in competitive harm. For example, an employee that misappropriates marketing plans, product plans, details about customer purchases or purchasing plans, potential acquisitions or partnerships and the like can create enormous harm to a company. The consequences might include loss of sales continuity, loss of sales contacts, a reduction in the sales pipeline, cancelled contracts and lost revenue.

OTHER CONSEQUENCES

There can be a variety of other consequences that arise from employees exfiltrating data from their employers. For example, an organization that does not properly manage its data assets or monitor information flows may never fully understand what has been taken by former employees. In the absence of appropriate data inventory and management practices, employers might never be able to prove what employees have taken, when it was taken, and how it was exfiltrated. This can lead to investigations by regulators, government agencies and others who may subsequently investigate potential data breaches that the employer may never be able to address fully.

ESTABLISHING POLICIES AND PROCEDURES

To minimize or eliminate the potential for employees to exfiltrate data from their employer when they leave a company, there are a number of things that an employer can do to proactively address the problem:

- **Ensure ongoing visibility of sensitive corporate data**
  It is essential that organizations maintain complete, ongoing visibility of sensitive corporate data across all of their endpoints, cloud applications and any other repositories where this data might be stored. An important best practice to accomplish this is the deployment of a content archiving system that will enable the capture, indexing and immutability of content based on corporate policy. Email archiving is the logical and best first place to start the process of content archiving, but other data types – such as files, social media content, text messages, web pages and other content – should also be considered for archiving, as well.

To minimize or eliminate the potential for employees to exfiltrate data from their employer when they leave a company, there are a number of things that an employer can do to proactively address the problem.

- **Limit employee access to data**
  Companies should establish policies to limit employee access to sensitive and confidential data by role, function, need to know, etc., although they must be given access to the content they need to get their jobs done. For example, only rarely would engineering employees need to access data in CRM systems, nor would salespeople have a need to access HR data. While IT needs to be in control of corporate data, it should not have unfettered access to all information, such as sensitive HR files on employees, compensation, structural changes, etc. By limiting employee access to sensitive or confidential information, the potential impact of employees exfiltrating data can be mitigated. The use of solutions that will allow users to gain access to the content they need, but not more than they need, is essential.

- **Encrypt data in-transit, at-rest and in-use**
  Sensitive and confidential data should be encrypted in transit, at rest and in use, regardless of its location. While manual encryption should be implemented so that employees can encrypt sensitive content in email, for example, Osterman Research also recommends the use of policy-based encryption that will automatically scan content based on policy and then encrypt it appropriately. Encryption alone can prevent much of the data loss that occurs when employees leave a company.

- **Require appropriate authentication for sensitive content**
  Sensitive and confidential information should be protected with good authentication to prevent its access by unauthorized parties. For example, relatively benign sensitive data might require just a username and password for access, while more sensitive or confidential information might require two-factor authentication. Decision makers should also consider the use of risk-based authentication that will impose authentication commensurate with the sensitivity of the information being accessed, the location from which it is being accessed, the time of day it is being accessed, and other relevant parameters. In some cases, it may be appropriate to create policies that will alert, or require approval from, a compliance officer when certain types of data are requested.

- **Manage mobile devices and laptops properly**
  Because of the significant amount of data stored on smartphones and laptops, it is vital that every mobile device can be remotely wiped so that former employees no longer have access to the content stored on these devices. This is particularly challenging in Bring Your Own Device (BYOD) environments, since corporate data may be stored on personally owned devices using non-approved approved applications, and IT often will not have the ability to remotely wipe these devices, allowing ex-employees to retain access to corporate data. It is important to note that enterprise-approved apps and any associated offline content can be remotely wiped, even if the device is personally owned.

- **Ensure an effective backup policy**
  Every organization needs an effective backup policy to ensure that all corporate data is backed up, preferably to a central or easily accessible location. However, this is becoming increasingly difficult because of the use of personally managed file sync and share tools like Dropbox, as well as other cloud repositories. While IT has the ability to properly back up all of the systems to which it has access, a significant proportion of corporate content, when stored in personally managed repositories, is not under IT's control.

  The research conducted for this white paper found that fewer than three in five organizations has a backup and recovery solution to ensure that data can be recovered if an employee maliciously changes or deletes data prior to informing the company of his or her departure. It is important to note that Office 365, as well as most cloud application providers, do not provide backup and recovery services in a holistic manner, and so organizations can have a false sense security about the data that is managed by their end users.

Sensitive and confidential data should be encrypted in transit, at rest and in use.

- **Insert clear confidentiality provisions in employment contracts**
  Employment contracts and agreements should include clear language about the provisions for protecting sensitive and confidential data while employees are working for a company, as well as when they leave. While these provisions may be disputed by employees after they leave a company, or may be disregarded altogether, employers at least have some basis on which to defend a position if they decide to pursue non-compliant ex-employees.

- **Develop policies on proper use of platforms**
  It is essential that all organizations have acceptable use policies regarding the proper use of corporate email, company-owned computers and mobile devices, personally owned computers and mobile devices, cloud applications, mobile applications, file sync and share tools, and any other platform where corporate data might possibly be stored. Employees should be trained on these policies and asked to sign an acknowledgement that they understand them.

- **Adopt policies to monitor and audit employee behavior**
  Organizations should adopt policies that will inform employees of management's intent to monitor and audit employee behavior when using any corporate resource, such as a computer, mobile device or network; and when using any corporate data resource. The goal of monitoring and auditing is to enable insight into how employees are accessing data and what they are accessing, as well as to deter potential misbehavior.

- **Conduct employee training policies**
  Employees should be well trained about all company policies, particularly those that deal with sensitive or confidential data assets. Training should include information about the devices, applications, networks and other resources that can and cannot be used to access corporate data resources, particularly those that are sensitive or confidential. However, the research conducted for this white paper found that only 68 percent of the organizations surveyed provide any educational programs for employees about digital security awareness and the definition of company intellectual property.

- **Do not allow employees to become their own administrators**
  It's rarely a good idea to allow employees to have administrative rights for their own, company-supplied computers, since this permits them to install applications that may permit the storage of corporate data in locations outside of IT control. Moreover, allowing employees to install applications, mobile apps and the like may increase the likelihood that employees will introduce malware, ransomware or other threats into the corporate network. It's important to understand that many cloud productivity tools, such as Microsoft OneDrive and Google Drive, permit employees wide latitude over the data they store, edit and delete in these repositories without any oversight from IT.

- **Do not attach printers to single computers**
  It is best practice not to attach printers to standalone computers, since this can allow an employee to print sensitive or confidential data before his or her departure from the company without the ability for administrators to monitor printing activity. Use of network printers, while not a foolproof way to prevent the theft of information, can allow print jobs to be monitored by administrators.

- **Determine who "owns" social media contacts**
  One of the key benefits of social media tools like Twitter is that it allows companies and individuals to establish themselves as industry experts and develop a base of followers. One of the key problems, however, is determining who "owns" these followers: the employee whose posts were attractive enough to engage these followers, or the company who employed him or her. That decision needs to be made long before an employee begins posting on behalf of the company.

Employment contracts and agreements should include clear language about the provisions for protecting sensitive and confidential data.

- **Train managers properly**
  Managers need to be trained properly and on an ongoing basis to be aware of the various issues involved when employees leave and how to handle exiting employees professionally to prevent both inadvertent and malicious loss of data. This training must be a regular practice so that managers can remain current on changes in employment law and on best practices for dealing with employees.

IMPLEMENTING THE RIGHT TECHNOLOGIES

Protecting sensitive and confidential data assets from exfiltration by departing employees is not just a matter of implementing the right policies, but instead combining good policies, best practices and the right technologies into a solution that will mitigate or eliminate the potential for improper conduct by departing employees.

CONTENT ARCHIVING

As noted earlier, content archiving is an essential component of any organization's data protection capability. Because archiving can capture, index and make corporate data tamper-proof, it allows data managers the opportunity to retain, search for and appropriately manage data assets. Most organizations begin archiving with email because it represents much of the sensitive and confidential data that organizations possess, but decision makers should also seriously consider archiving other content types, including social media posts, text messages, web meeting content, voicemails, visitor logs and any other content that contains a business record.

It is important to note that while archiving is a key best practice to protect corporate data, a corporate archiving system cannot capture data if it is under the sole control of employees. For example, an employee who maintains corporate data in a personally managed file sync and share account and uses personal devices can create, modify and delete content independently of the corporate systems whose content will be archived.

In a similar vein, organizations should deploy a centralized endpoint and cloud application backup solution that will capture all relevant data as part of a regular backup routine. This protects the company to ensure that data is recoverable if an employee steals a device, or if he or she deletes data. It is important to note that archiving and backup are not substitutes for one another, but both are best practices that every organization should implement.

The research conducted for this white paper has found that many organizations are not even saving basic data types when employees leave, as shown in Figure 2.

The research conducted for this white paper has found that many organizations are not even saving basic data types when employees leave.

Figure 2
Data Types That are Retained When Employees Leave an Organization

Content	Always	Sometimes	Never	N/A
Files managed by the employee (e.g., on a file server)	52%	36%	7%	4%
Emails	51%	42%	4%	3%
The MyDocuments folder (or equivalent) on the employee's laptop	33%	48%	15%	5%
Calendar data	33%	38%	27%	2%
Contact data	32%	40%	25%	3%
The MyDocuments folder (or equivalent) on the employee's desktop	31%	50%	14%	5%

Figure 2
Data Types That are Retained When Employees Leave an Organization (concluded)

Content	Always	Some-times	Never	N/A
Data on the employee's company-owned smartphone	27%	30%	30%	13%
Data on the employee's company-owned tablet	26%	28%	27%	18%
Data in OneNote	17%	20%	29%	34%
Data in OneDrive	16%	28%	17%	39%
Skype for Business/Lync data	12%	18%	37%	33%
Corporate data on the employee's personal smartphone	12%	25%	48%	15%
Data in other file sync and share tools (e.g., Dropbox)	11%	29%	27%	33%
USB sticks that had been used by the employee	10%	38%	39%	13%
Corporate data on the employee's personal tablet	9%	24%	50%	17%
Yammer data	3%	11%	32%	54%

Source: Osterman Research, Inc.
Note: totals may not add to 100% because of rounding error

It is important to note that the list of data types in the table above is not exhaustive. For example employees can also take with them SharePoint data, Salesforce data and a wide variety of other corporate systems when they leave a company.

ENTERPRISE CONTENT MANAGEMENT

Enterprise Content Management (ECM) is a set of processes and solutions designed to capture, manage, archive and deliver unstructured, semi-structured and structured information to individuals and business processes. The fundamental purpose of ECM is to provide users with the information they need within the context of a content management solution that will manage all data types holistically, eliminating the siloes of information that most organizations must manage today. ECM solutions are useful in preventing data theft from departing employees because they provide decision makers with the ability to control access and understand where their corporate data resides.

The fundamental purpose of ECM is to provide users with the information they need within the context of a content management solution that will manage all data types holistically.

VIRTUAL DESKTOPS

Virtual desktops are another way to reduce the likelihood of departing employees from exfiltrating sensitive or confidential information before they leave. Because no data is stored locally, virtual desktops are a useful technology that will make it more difficult for employees to misappropriate data, such as by copying it to a USB drive or by stealing a hard drive full of data, since virtual desktops house no local data.

WINDOWS TO GO DRIVES

Windows to Go Drives are another useful technology that permits IT to have more control over data access. Windows to Go is supported under Windows 8 and 8.1 Enterprise, Windows 10 Enterprise and Windows 10 Education. It allows administrators to build a complete Windows environment on a USB drive and allows users simply to plug the drive into any compatible PC (or Mac) and have a full Windows experience on that platform. Windows to Go provides administrators with much more control over the user experience and can be managed using group

policies, preventing installation of non-approved applications.

ENCRYPTION

In organizations that have not fully embraced or deployed encryption, perhaps the place to begin the process is by targeting the areas that are most obviously in need of protecting sensitive or confidential content: sensitive data assets and the devices that are used to access them. Decision makers should identify privileged communications, as well as content that could greatly harm the company's standing with business partners and other key constituencies if it was exfiltrated by departing employees. This includes files that contain clearly sensitive documents like financial projections, draft policy statements, bids, tenders, acquisition information, employee medical records, partner information or customer financial information. This content typically represents the vast majority of the risk in most companies and is relatively easy to protect using robust encryption technologies.

MOBILE DEVICE MANAGEMENT

Mobile Device Management (MDM) technology can protect corporate data on mobile devices by allowing an administrator to monitor content on corporate and personally owned devices, containerize corporate data on personally owned devices, and remotely wipe this data quickly. While it's possible for an employee to exfiltrate data from mobile devices before they have announced their departure, MDM solutions ensure that employees will not have access to corporate data on mobile devices after their access is supposed to end.

The research we conducted for this white paper found that only 43 percent of organizations use an MDM solution to delete enterprise apps from BYOD devices, 19 percent simply trust employees to delete corporate information from their personal devices, and 14 percent have no way of deleting enterprise apps and content.

The research we conducted for this white paper found that only 43 percent of organizations use an MDM solution to delete enterprise apps from BYOD devices.

EMPLOYEE ACTIVITY AND CONTENT MONITORING

Another important technology to help prevent employee exfiltration of data are solutions focused on monitoring employee activity and how content is accessed. There are varying levels of features and functions for the variety of monitoring tools currently available, but capabilities enabled include monitoring all email and webmail traffic, tracking the web sites that employee visit, capturing all of their instant messages and social media posts, logging the files they have accessed, taking periodic screenshots, and even keystroke logging in some cases. While these types of tools carry with them a bit of a "creepiness" or "Big Brother" factor, they are useful in two ways: first, by allowing IT to understand just about everything an employee is doing; and second, by inhibiting inappropriate behavior because employees know their activities are being tracked.

IMPLEMENT DLP AND/OR FILE ANALYTICS TECHNOLOGY

Another useful set of capabilities to protect corporate data are Data Loss Prevention (DLP) and file analytics tools. DLP tools monitor content and can carry out a variety of actions based on pre-determined policies. For example, if an employee attempts to download sensitive or confidential information to which he or she would not normally have access, or if an employee downloads a large amount of information, the request can be sent to a compliance officer for approval. Our research found that only 56 percent of the organizations surveyed for this white paper have a DLP solution in place.

File analytics technology allows administrators and others to search through unstructured data that can be stored just about anywhere across an enterprise, analyze the content of this information, apply supervisory rules, and retrieve information as needed. File analytics tools can scale massively to allow search, analysis and retrieval of enormous volumes of information.

SOLUTIONS THAT WILL PREVENT OFFLOADING OF DATA

Another useful technology that can reduce the likelihood of employees exfiltrating data upon or before their departure is the ability to prevent the copying of data onto physical media, such as CD-ROMs, DVD-ROMs or USB drives. Depending on the technology, these can be controlled by policy so that employees with a legitimate need for these capabilities can perform these functions, but all others will not be able to do so.

CENTRALIZED LOGGING AND REPORTING

Another important capability is centralized logging and reporting of employee activity so that administrators know which files are being accessed, who is accessing them, when they were accessed, the devices on which they were stored, etc. Centralized logging and reporting not only allows investigators to conduct forensic analysis to track where files were copied and by whom, but employee knowledge of these capabilities might inhibit inappropriate behavior by departing employees.

REPLACE BYO SOLUTIONS WITH IT-MANAGED ONES

BYO is a fact of life in most organizations and IT has accepted/embraced/acquiesced to the idea that employees are using their own devices, applications and tools to access and process corporate data. The fundamental problem with BYO is not one of intent – the vast majority of employees really are trying to be more productive and efficient by using tools that either are not supported by IT or that IT cannot afford to provide to employees. The result is that employees are now in charge of many of the tools they use on a daily basis, and in primary control of the data that is processed by these tools. That creates problems for an organization in the context of compliance, legal considerations, and best practices around protecting and managing data.

Osterman Research has recommended for quite a long time that IT departments determine the BYO tools that employees are using, establish why employees use these tools instead of IT-managed capabilities, and then offer alternatives that will put IT back in charge of the data management process. The key is to provide a tool that is just as easy to use as the personally managed tools that employers are seeking to replace and with an interface that users will want to employ, but that allows IT to be in control of where data is stored.

OTHER CONSIDERATIONS

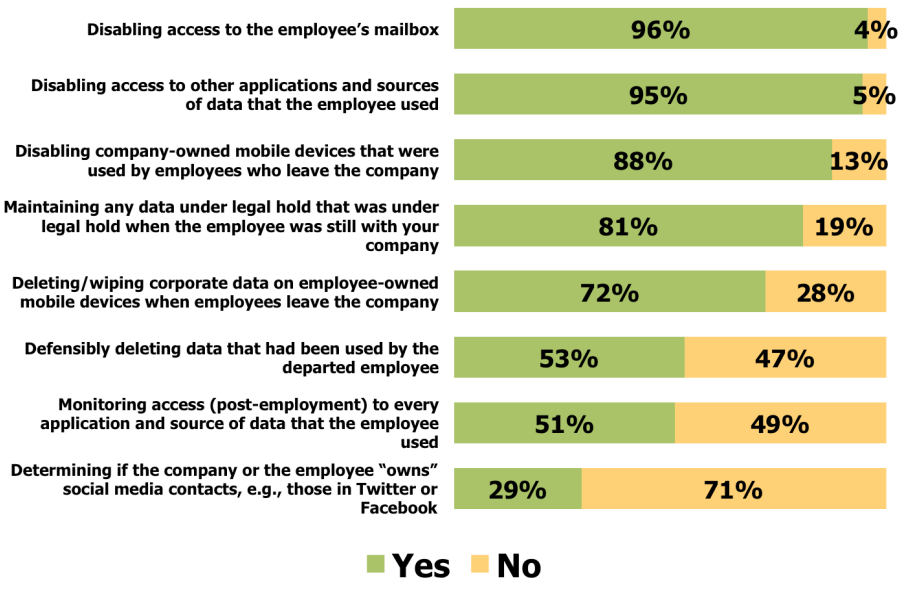
It is important for companies doing business in the European Union (EU) to look for solutions that help them comply with the General Data Protection Regulation (GDPR), as well as solutions that support workflows that will help them conduct efficient, cross-border eDiscovery. Centralized platforms that address key objectives of cross-functional teams like IT, information and legal can also be useful to mitigate the risk of employees altering or deleting data when they leave a company.

It is important for companies doing business in the European Union to look for solutions that help them comply with the General Data Protection Regulation.

A CHECKLIST FOR MANAGING THE EMPLOYEE DEPARTURE PROCESS

Osterman Research has developed a checklist that decision makers should consider in order to manage the employee departure process and protect the data to which they have access. Our research has found that many organizations do not have well-established processes and systems in place to manage the employee departure process, as shown in Figure 3.

Figure 3
"Does your company have a well-established process and systems with which all relevant decision makers in your company are familiar?"



Source: Osterman Research, Inc.
Note: totals may not add to 100% because of rounding error

PHYSICAL ACTIVITIES

- Obtain custody of the employee's company-supplied computers and mobile devices, as well as all external hard drives, thumb drives, backup discs, etc. The research we conducted for this white paper found that 25 percent of the organizations surveyed never require departing employees to sign a document indicating they have returned all corporate data assets.

- Obtain custody of company credit cards, security access cards, parking codes, etc.

- Take an inventory of all of the files or projects on which the employee was working, and make sure that all such materials have been returned. This is particularly important for employees who work remotely.

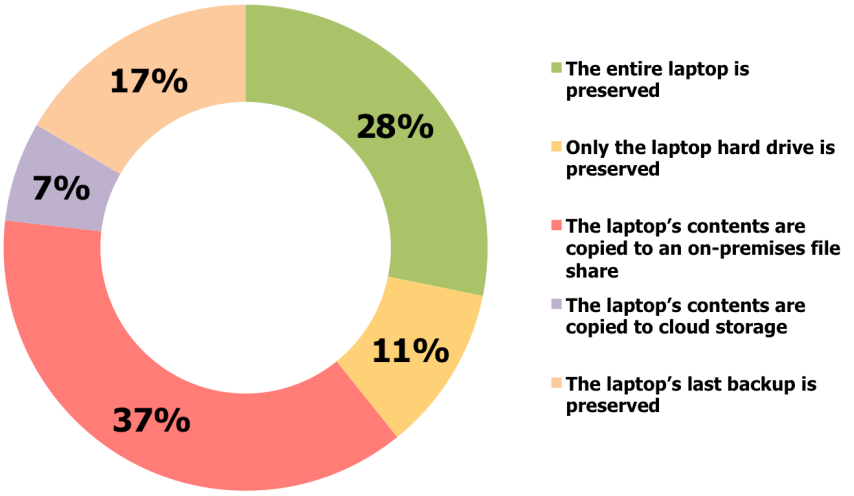
- During the exit interview ask the employee questions about future plans/employment to determine potential risk.

- Give managers access to their employees' content archives.

As shown in Figure 4, organizations employ a wide range of activities with regard to retaining content on employees laptop computers (the survey results show that these practices are virtually identical for desktop computers).

During the exit interview ask the employee questions about future plans/ employment to determine potential risk.

Figure 4
Procedures for Processing Laptop Computers When Employees Leave



Source: Osterman Research, Inc.

ACCOUNT ACTIVITIES

- Disable all accounts to which the employee has access. A 2015 SailPoint survey found that 66 percent of employees had access to corporate data that they had uploaded to a cloud storage application like Dropbox *after* they left their employer – one in five employees have uploaded this data specifically for the purpose of sharing it outside of the company[xiii].
- Disable access to the company network.
- Disable access to the Active Directory user account or equivalent.
- Change passwords for all applications, cloud-based storage, etc.
- Take the employee's security pass.
- Remove employee from all distribution lists.
- Redirect employee communication (e.g., email) to an appropriate individual.
- Delete the employee's voicemail account and/or change the voicemail password.
- Ensure that when an employee leaves the organization, his or her email is forwarded to someone else, such as the departed employee's manager or replacement. Our research found that only 36 percent of organizations always do this, while another 53 percent do so only in some instances.

OFFICE 365-SPECIFIC ACTIVITIES

- Disable the employee's Office 365 user account.
- Change Office 365 account access and select a new user for this account.
- Analyze the quantity of data by type.
- Select the data to preserve from the user's account.

A 2015 SailPoint survey found that 66 percent of employees had access to corporate data that they had uploaded to a cloud storage application like Dropbox after they left their employer.

- Copy data to an appropriate archive, select the location for it, and ensure that the data can be restored indefinitely.
- Place the Office 365 mailbox on legal hold.
- Install the desktop Agent.
- Copy files from file shares.

BACKUP, ARCHIVING AND CONTENT MANAGEMENT FUNCTIONALITY

- Reduce storage cost using low-cost, cloud-based, 'cool' storage (storage designed for the retention of data that is rarely accessed).
- Deploy backup and recovery solutions that are designed for rapid restoration of files if employees delete or corrupt files.
- Keep compute charges low with on-demand indexing and search.
- Implement automated retention and disposition policy management capabilities.
- Implement ECM capabilities that will provide users with the ability to access and make changes to existing documents, but that will do so under the control of corporate policies focused on appropriate roles and permissions and that will provide a thorough record of all file transactions. This includes activities by mobile users, users of enterprise file sync and share systems, and all other corporate solutions.
- Implement a permanent locking feature for SEC compliance.
- Implement secure data wiping for DoD compliance.
- Implement file/document fingerprinting for data integrity and compliance.
- Implement a legal hold feature to prevent disposition of data.
- Do a full text search of data with wild cards and Boolean operators.
- Save any searches to preserve search results.
- Implement case management capabilities in order to manage different sets of searches.
- Implement user access control to allow controlled access to archives.
- Export search results in standard formats (e.g. .csv, .pst, EDRM).

MANAGEMENT ACTIVITIES

- Provide good training for managers so that they can be aware of best practices for managing employees, recognizing problems before they occur, dealing with departing employees, and handling exits professionally.
- Providing good training for employees so that they are aware of best practices for protecting data, using company-approved tools, and maintaining adherence to company policies.
- Create a positive work environment, including treating employees with respect, in order to minimize the potential for malicious theft of corporate data resources.

Deploy backup and recovery solutions that are designed for rapid restoration of files if employees delete or corrupt files.

- Implement the appropriate solutions that will allow HR, senior executives, legal and other relevant parties to monitor managers' behavior so that they can identify managers who need additional training on how to deal with employees in a professional manner.

OTHER ACTIVITIES

- Monitor employee activity for suspicious behavior, security breaches, etc.
- Retain all employee files and other information for potential audits or investigation.
- Wipe clean personal devices used for work as permitted by company policy.
- Remove any rights the employee may have had regarding the organization's domain name(s).
- Remove any rights the employee may have as administrator of the organization's Web site and extranets.
- Remove employee references on the company Web site.

SUMMARY

Employee turnover is common, as is the practice of employees taking sensitive and confidential data with them when they leave, particularly data that they were involved in generating. This creates a significant risk for employers whose data was misappropriated, resulting in potential data breaches that can trigger regulatory actions or legal actions, as well as a variety of other consequences. Most employers are not adequately prepared to deal with the aftermath of employee data theft and many do not take the steps necessary to mitigate these risks before they occur. However, there are a number of things that decision makers can do to protect their companies and minimize, if not eliminate, the threat of employee theft of sensitive and confidential information. These include creation of corporate policies focused on appropriate employee management of data, establishment of processes designed to control employee use of data, and deployment of technology solutions that will protect corporate data to the greatest extent possible.

SPONSOR OF THIS REPORT

Archive360 is the market leader in email archive migration software, successfully migrating more than 12 petabytes of data for more than 500 organizations worldwide since 2012. The company's flagship product, Archive2Anywhere™, is the only solution in the market purpose-built to deliver consistently fast, trouble-free, predictable archive migrations, with verifiable data fidelity and defensible chain of custody reporting. Archive360's newly released Archive2Azure solution is the industry's first regulatory compliance and grey data storage solution based on the Microsoft Azure platform. Archive360 is a global organization that delivers its solutions both directly and through a worldwide network of partners. Archive360 is a Microsoft Cloud Solution Provider and the Archive2Azure solution is Microsoft Azure Certified.

ARCHIVE360
POINT. CLICK. MIGRATE. STORE.

www.archive360.com
@Archive360
+1 630 358 4448
info@archive360.com

REFERENCES

[i] http://www.darkreading.com/vulnerabilities---threats/survey-when-leaving-company-most-insiders-take-data-they-created/d/d-id/1323677?&utm_ source=press%20release&utm_ medium=blog&utm_campaign=dotd%20survey

[ii] https://www.sailpoint.com/uploads/files/general-files/MPS-2014-Infographic-v2.png

[iii] http://www.wsj.com/articles/u-s-bank-regulator-notifies-congress-of-major-data-security-breach-1477684445

[iv] http://www.payscale.com/data-packages/employee-loyalty/full-list

[v] http://www.bls.gov/news.release/tenure.nr0.htm

[vi] http://www.informationweek.com/strategic-cio/10-top-tech-companies-poised-for-massive-layoffs/d/d-id/1325015

[vii] http://oilprice.com/Energy/Energy-General/After-350000-Layoffs-Oil-Companies-Now-Face-Worker-Shortages.html

[viii] http://money.cnn.com/2016/12/05/technology/expedia-hack-insider-trading-sec/index.html

[ix] http://www.law360.com/articles/689244/plumbing-co-says-rival-stole-trade-secrets-employees

[x] http://www.smh.com.au/business/bluescope-steel-stung-by-alleged-corporate-espionage-20160107-gm1f0j.html

[xi] http://www.ventkerlaw.com/wp-content/uploads/2015/12/Atlantic-Marine-v-McGrath-Trade-Secret-case.pdf

[xii] http://www.shandtaylor.com.au/publications/theft-of-confidential-information-costs-employee-50000

[xiii] https://www.sailpoint.com/2014marketpulsesurvey/