Preventing Data Theft by Departing Employees

When employees leave a company, there is a heightened risk of data theft, which is also known as data leakage or exfiltration. This risk is present whether an employee's departure is voluntary or not.

The consequences of data theft from insiders can be severe, as an organization's most valued data assets and secrets are vulnerable. Data leakage events can impact a company's financials through lost business and intellectual property, and they can result in reputational damage, litigation and regulatory fines.

Departing employees may have various motives for stealing sensitive corporate data, and it is crucial to be aware of and look for warning signs that an insider may engage in this impropriety. This article offers more information on warning signs and provides actions businesses can take to help prevent these occurrences.

Reasons Sensitive Data May Be Stolen

There are several reasons departing employees may take corporate data. While some may have malicious intent, other incidents may be the result of accidents or misunderstandings. The following are common reasons a departing employee may take corporate data:

- **To secure a new job or compete with a former employer**—A company's trade secrets or intellectual property can be valuable to a competitor. A departing employee may leverage this data to obtain a new job or gain an advantage in a new position by using it to compete with their former employer.
- **For personal financial gain**—A former employee may be able to sell data they take, or they may be able to use it to jumpstart their own business venture.
- **To seek revenge**—Departing employees may be disgruntled or frustrated about the circumstances of their transition. This may lead to malicious destruction of data to sabotage or disrupt their previous company's operations.
- **On accident**—Data exfiltration may not always be the result of malevolent actors. Departing employees may incorrectly believe the data was theirs, or they may accidentally retain it by failing to sufficiently wipe the devices they used for business purposes.

Data Theft Warning Signs

Companies can work to prevent data theft by proactively monitoring warning signs. Indicators that an employee may compromise sensitive information include actions such as:

- Engaging in suspicious web-based activities, including utilizing incognito browsers, having several webmail accounts, researching how to bypass security and using personal file sharing platforms
- Using unauthorized personal devices for business activities
- Accessing business data at unconventional times or repeatedly
- Downloading or transferring an inordinate amount of data
- Requesting to gain access to information that is outside the scope of their job description
- Recording or taking screenshots of company meetings
- Acting out of character or in a way that is against company policies
- Trying to trick or pressure coworkers into gaining access to their data

Prevention Tips

Organizations can implement the following strategies to reduce the risk of departing employee data theft:

- **Be proactive**. Look for warning signs to stop data theft before it happens.
- **Establish clear policies and procedures**. Policies should state the delineation between personal and business use of data, devices, networks and other technologies. They should also contain procedures on how this information will be disseminated to new, existing and departing employees.
- **Assign ownership of insider threat risks**. Designate someone within the organization to be responsible for updating the data theft prevention program, conducting employee trainings and maintaining a data theft incident response plan.
- **Have a zero-trust mindset when employees leave**. Assume a departing employee will retain some access to sensitive information after they leave. Utilize tools that create a full audit trail should an issue arise.
- **Acknowledge that no system will be completely effective in stopping all data theft**. No matter how advanced, technological data loss prevention systems are not capable of preventing all instances of data exfiltration. Continually update your policies and regularly test your procedures.
- **Encourage cross-collaboration between business units (e.g., HR and IT)**. This can be particularly useful during offboarding to ensure equipment is returned in a timely matter and departing employee access to data is restricted when necessary.

Data theft from departing employees presents a significant exposure, and companies must be aware of warnings signs and techniques to mitigate its associated risks. For more risk management guidance, contact us today.
