Enterprise Security Tech Q&A with Andreas Mueller, founder & COO of Downstreem LLC

Apr 11

Experts Warn of the Ramifications of Tech Layoffs, Including Data Security and Legal Concerns

As the tech industry continues to experience a wave of layoffs, experts predict that there will be a surge in conflicts and litigation over intellectual property theft. This concern is not limited to social media or email accounts but extends to the personal phones of former employees. With access to company data and trade secrets, former employees could potentially steal valuable intellectual property and use it for their own gain or to benefit a competitor. Such actions could result in costly legal battles for companies trying to protect their intellectual property. The importance of safeguarding intellectual property during layoffs cannot be overstated, as it could have a significant impact on a company's future success and competitiveness in the market.

We spoke with Andreas Mueller, COO at Downstreem about the potential backlash organizations could face during layoffs and what they can do to implement safe layoff protocols to ensure corporate data security.

Can you explain the current trend of big tech layoffs and why you predict a potential backlash in terms of intellectual property theft?

Since the start of the year, we have seen tech lay off over 120k people, citing economic concerns and a changing market as reasons behind the layoffs. Anytime employees leave or are asked to leave a company, there is a risk of backlash, which can be especially harmful to companies if the backlash is in the form of proprietary information theft.

When stability is threatened, often we see this play out with cascading departures to other organizations and a shift in corporate culture. Big tech companies require constant communication to operate efficiently. Huge disruptions to operations can lead to low morale for former employees and existing employees struggling to maintain work.

With the sudden departure of employees and thousands who have already been laid off, several individuals with intrinsic knowledge of the company's internal development and operational flow will likely seek employment in similar positions with competing companies or possibly start companies of their own. As smaller rivals look to gain leverage, they will likely seek out these recently disgruntled employees to help expand their operations.

How does mobile data theft play into the issue of intellectual property theft during corporate layoffs, and why do you think this aspect is often overlooked?

Employees regularly communicate and conduct work through mobile devices making mobile data critical to most organizations. Especially during the pandemic when remote work became necessary, mobile data became even more prevalent. However, the shift to mobile and remote work has also made it difficult for companies to monitor and control data use.

Technology teams had to adapt to mobile device management (MDM) solutions, which was difficult to control from a data dependency standpoint. Many organizations struggled to adapt to different MDM solutions, and some employees used corporate data on their personal devices, which exacerbated the risk of intellectual property theft.

This shift made it difficult for companies to monitor and log data use. During events such as employee departures, it's a challenge to manage data on personal mobile devices since they often retain large amounts of corporate data, such as emails, contact information, and attachments.

During corporate layoffs, intellectual property (IP) theft is often done through a mobile device, but frequently overlooked. The lack of oversight and control over employees' privately owned devices can lead to the loss of sensitive information, and the risk of it later being used by competitors.

What are some examples of the types of data that are commonly stolen from mobile devices during layoffs, and how does this affect the affected companies?

During layoffs, there are several types of data commonly stolen from mobile devices. The first type is intellectual property, which often constitutes a company's most valuable asset, including patents, copyrights, and trademarks. Another data type includes personal information of employees or customers, which may entail names, addresses, social security numbers, and financial data. Other common data includes company financial data, business plans, product development information, and customer lists.

The theft of data from mobile devices during layoffs can have serious consequences for organizations. Companies can lose revenue or market share, face reputational damage, and legal consequences.

Can you speak to the importance of implementing an employee departure protocol to prevent intellectual property theft during layoffs, and what should be included in such a protocol?

Implementing an employee departure protocol is crucial to preventing IP theft. A departure protocol can help minimize risk and protect the company's valuable assets, especially during layoffs.

There are five major aspects of departure protocol to consider. First, conduct an exit interview with the employee to discuss any confidential or sensitive information they may have access to and ensure that they understand their obligations to protect the company's IP. Second, immediately disable the employee's access to all company systems, including email, databases, and other IT systems. This can help prevent unauthorized access to company information. Then, retrieve all company property, including laptops, mobile devices, access cards, and any other company-owned items in the employee's possession. After any company property has been retrieved, review the employee's files to ensure that all confidential and sensitive information is removed or secured. Finally, monitor the employee's access to company systems after their departure to ensure that there is no unauthorized access.

What can companies do to better equip themselves to find and protect their stolen intellectual property, particularly when it comes to mobile data and messaging apps?

Protecting a company's intellectual property (IP) has always been a major concern for companies. The increasing use of mobile devices and messaging apps has created new challenges for companies to protect their IP, but there are steps they can take to address the issues related to mobile devices.

To start, they should have a comprehensive plan in place that includes policies, procedures, and technology solutions to protect their IP. This should include implementing encryption and access controls to ensure that data cannot be read or intercepted by unauthorized parties. Companies should also monitor and audit mobile device usage to prevent unauthorized app usage or data sharing through messaging apps. Additionally, it is vital to educate employees on IP protection and provide training on how to handle sensitive information, including mobile data and messaging apps. Conducting regular security assessments can also help identify vulnerabilities and ensure that the IP protection plan is up-to-date and effective. Finally,

companies can leverage legal measures, such as registering trademarks and copyrights, and taking legal action against those who steal their IP.