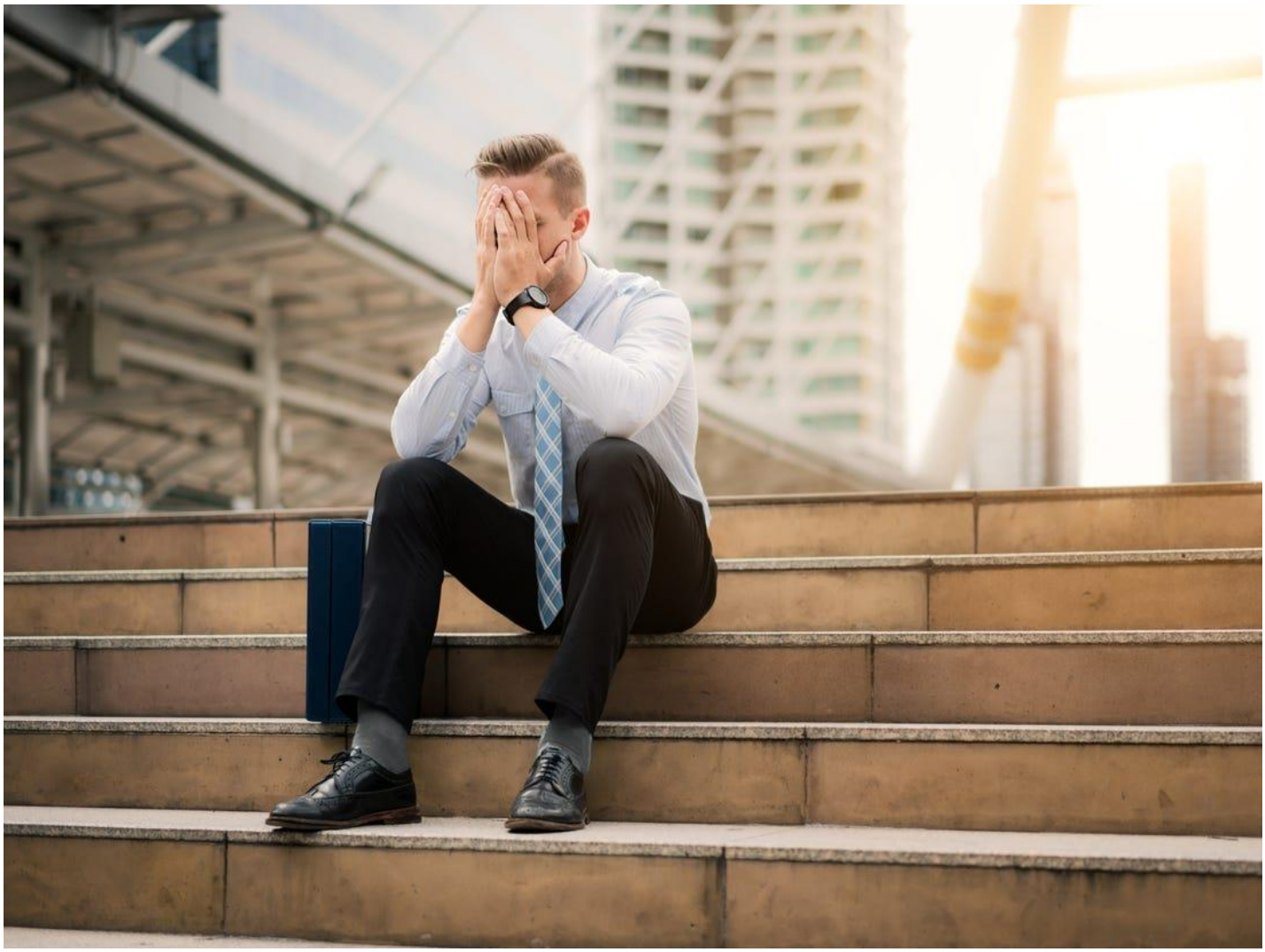
The Risks Of Employee Layoffs And What You Can Do About It?



"When you are in a small boat, you can see who's paddling hard and who's looking around."

- *Ev Williams*

Let me start with a story about a former cisco engineer…

An ex-Cisco engineer broke into Cisco systems without the company's permission. **The incident occurred five months after he resigned** from his position as an engineer at Cisco.

During his unauthorised access, he admitted that he deployed a malicious code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing and other collaboration tools.

As a result of this incident, the 16,000 WebEx Teams accounts were shut down for up to two weeks, which caused Cisco to spend approximately $1.4 million to restore the damage to the application and refund over $1 million to affected customers. In total the damages re

The incident points to a serious insider threat security concern for organisations, specifically to those employees who have left the organisation in "bad terms".

The Covid-19 pandemic is triggering layoffs in nearly every business sector. In the US, more than 1 million Americans continue to apply for jobless benefits every week.

Many countries have placed severe lockdown on businesses. In Australia, Victoria State has been locked down for over two months.

Call it realism or pessimism, but many businesses won't survive and not just because of the mass shutdowns.

As companies lay off thousands of people, they put themselves at risk of losing critical data because former employees can walk out the door with sensitive customer information and private records.

Tough times require harsh measures, and layoffs are one of them. Yet many organisations make matters even worse by handling layoffs poorly without realising the potential consequences.

What are the risks when employees leave?

Data Exfiltration: When employees are laid off, the relationship between the employee and the organisation can be soured. This could motivate them to take data with them.

Data Loss: When employees are laid off, they can take it too personally and vent their anger and disgruntlement. If the former employee still has access to systems as well as data, they could intentionally delete or damage files they know to be critical to the business, often referred to as "sabotage".

Data Leak: When employees are laid off, they could accidentally leak sensitive data that they have access to as a result of their negative and emotional state that they find themselves.

Suggested Recommendations

To prepare for an employee departure, organisations must address several areas before the employee's last day.

A terminated checklist can help you track the various steps an employee needs to complete. The checklist can include the following:

- **Manager**
    - Ensure an exit interview is scheduled by the next higher-level manager or HR. Provide final performance appraisal
- **Finance Department**
    - Ensure that employee returns company credit cards and close accounts
- **The IT Security Department**
    - Terminate all accounts (VPN, email, network logins, cloud logins and any specialised access). Also, change privileges access for any shared accounts and network devices.
- **ICT Department**

    - Ensure that employee returns any company-owned equipment such as laptops, smartphones and other devices. Verify against inventory.
- **Physical Department**
    - Collect identification badges, keys, access cards, parking pass and so on. Verify against inventory and provide security briefing
- **Records Department**
    - Ensure that employee returns company-owned or controlled documents, books and any other information
- **HR Department**
    - Notify organisation of separation. Otherwise, employees may unintentionally disclose sensitive information to a former colleague and open themselves to social engineering attacks.
    - Reaffirm an IP and non-disclosure agreements. This is an opportunity to remind the employee of their obligations to the organisation even after separation.

Important: Apart from the checklist, most insiders steal IP within 30 days of leaving an organisation. You should therefore consider a more targeted monitoring strategy for employees and contractors when they give notice of their exit. The time frame should encompass 60-day window - 30 days before turning in their resignation and 30 days after.

This review should include email or any other online activities to ensure that the employee has not emailed sensitive company data outside the organisation

Uncover The Risk & Security Blind Spots In Your Organisation

Are you interested in identifying risky behaviour by your employees or other trust partners?

We can provide you with the visibility and insights you need to fully understand how users interact with company data.

Now, with an Insider Threat Assessment, we can provide you with insights in a limited 30-day engagement and get one report assessing your organisation and its most significant risks.

- We will provide you with the visibility and analytics, allowing you to understand where your data is living, how your users interact with it, and where and how it's leaving the organisation. You'll also get an understanding of how users behave both on and off the corporate network.
- Your assessment will also show whether your employees are circumventing security policies and controls.
- We will find and elevate your highest risk users for inspection and find out where you need to be investing your security resources to get the best results.

What is the process?

1. **Simple deployment** - We will deploy a specialised monitoring tool on the selected endpoint of your choosing. The agent is lightweight enough to deploy in mere hours and will have no noticeable performance impact.
2. **30 days of Collection** – We will monitor your endpoints, collect user activity data, and analyse that data
3. **Your Threat Report** - Once the 30-day data collection period is complete, we will review the findings and alerts and compile an executive summary & detailed report that highlights the most prominent risks on your organisation.

100% of Threat Assessments find some form of undetected, unaddressed security threat. Find out what's really happening in your organisation.

To request your assessment, please fill in the contact form: https://commsnet.com.au/contact-us or email us

Other Relevant Article & Videos

- **Financial Distress, A Key Motivation And likelihood To Commit Insider Harm** https://commsnet.com.au/resources/blog/93/financial-distress-a-key-motivation-and-likelihood-to-commit-insider-harm
- **Why The Coronavirus Outbreak Will Promote Insider Threats And What You Can Do About It?** https://commsnet.com.au/resources/blog/92/why-the-coronavirus-outbreak-will-promote-insider-threats-and-what-you-can-do-about-it
- **Why Organisations Miscalculate The Cost Of Insider Breach -** https://www.youtube.com/watch?v=4E8do-Q9p2w