# Mitigating The Accidental Insider Data Leak


***“Data by itself never walks out of the door!”***

Are you guilty of accidentally hitting the “**send**” **button** to the wrong person in an email or attaching the incorrect document? Don’t worry, you are not alone. We have all done it. We are ALL human. We make mistakes, that’s part of our DNA.

**Real case scenario**

A SCRIPT from Star Wars: **The Rise of Skywalker** was nearly leaked after a clumsy actor left it in their hotel room and it was listed on eBay.

The script was discovered by a cleaner and was then "given to someone else - who then went to sell it. According to Disney… luckily an employee saw it on eBay and bought it.

Not surprisingly, Disney notorious for its airtight, spoiler-proof security measures was not pleased with John Boyega's gaffe. Earlier this week, J.J. Abrams explained that the studio giant had distributed only "a handful of scripts, and they were printed on crazy, uncopyable paper." **But it took only one human error** for the coveted property, valued at about $84, to end up on an auction site.

**Human behaviour** offers many opportunities for mistakes to be made, especially by those rushing to complete multiple tasks in high-stress environments.

Beyond mistakes, high levels of stress in the workplace will either create an 'overwhelm' which put trusted assets into vulnerable states or those people will develop negligence behaviour.

The drive for productivity comes at a cost for both efficiency, accuracy and security. When employees are rushed, they will make more mistakes, feel as if their concerns are not being considered and potentially develop a negative attitude towards management.

Mistakes can be unintentional – anything from ignoring essential security control, speaking one's mind before understanding the repercussions, or accidentally sharing or leaking sensitive corporate information.

**So where does the responsibility lie to ensure organisation information is kept protected?**

A finding conducted by Gemalto in 2017 called Breach Level Index revealed that 76% of all the breaches occurred because of employee error. The worst part is that they could have been easily prevented.

For organisations to limit the number of insider data breaches, it's crucial for employees to understand the role they play in keeping the company's data secure.

Yet, it is essential to realise that it isn't practical for most organisations to implement 100% protection against every threat to your organisation assets.

That's why organisations need to adopt the following intention - **Employees are the first line of defence!**

Gone are the days when security was the sole responsibility of the corporate IT/security department.

Today, businesses need to consider threats from insiders whether they are malicious or accidental from a perspective of "enterprise-wide". Organisations need to develop a comprehensive risk-based security strategy to protect critical assets against the threats from inside and outside as well as trusted business partners.

Training employees to be the first line of defence doesn't mean that being security-minded in their online activities is sufficient. Organisations need to think and act beyond that.

## What can you do?

Organisations must understand the psychology of their workforce and the demand placed upon them by the leadership. Once these are understood, it's the responsibility of the organisation to create a work environment conducive to positive outcomes.

To reduce the likelihood of unintentional mistakes taking place, organisations may want to consider the following measures

1. **The means by which the levels of stress of employee can be reduced.**
    - May include helping employees focusing on achieving outcomes and mission-oriented objectives rather than activities.
    - May include in getting the organisation to focus on people-oriented rather than project-oriented management.

- May include in reviewing organisation corporate policies and procedures that make employee job easier but make it difficult for them to do something wrong (failure).
- May include time in work schedule to focus on tasks

2. **Awareness training that leads to responsible actions.** And while there is an evident and urgent need for better employee security awareness education, business leaders need to be doing more to provide employees with the ability and capability of being responsible for their actions.
    - Cyber awareness training that leads people from being aware of cyber threats and leading them to become cyber responsible - Getting insiders to act in the best interest of the organisation.
    - Insider threat awareness training which allows employees to be aware of their responsibilities to protect an organisation's critical assets (facilities, people, technology, information). For example
        - Understanding that employees can be targeted by a malicious individual as well as external adversaries
        - The ability to understand the consequences of being a malicious or unintentional insider.
        - Recognise how an employee can become an unintentional insider threat.
        - The ability to report behaviours not consistent with organisation acceptable behaviour.
3. **Hire new candidates with values that align with the organisation values**. Establishing and maintaining a "keen and happy" workforce will reduce the likelihood of unintentional incidents taking place.
    - Begin with hiring the right staff. Congruence of values between employees and the organisation promotes a strong culture. A high level of congruence will show up that "people care" and are less likely to perform the accidental incident

- However, if employee values become misaligned with the organisation values, the person should be respectfully but expeditiously ushered out of the organisation.

4. **Seek To Build Positive Culture**. The most powerful mitigating factor is a well-cultivated culture of peer networks that both support individuals as well as create expectations of excellence.
    - Focus on collaboration. A positive culture facilitates social interaction, teamwork and open communication. This collaboration can lead to some fantastic results.
    - Focus on job satisfaction. Employers who invest in the well-being of their employees will be rewarded with happy and dedicated employees.
    - Focus on employee wellness. Employees need to feel their best – physically, mentally and emotionally to contribute to a positive culture.
    - Focus on the organisation "meaning". Meaning and purpose are more important in the workplace now than ever. A majority of employees crave meaning and purpose in their work. It provides them with a reason for their contribution to the greater good of the organisation.
    - Encourage positivity. To build a positive culture, employers need to start by encouraging positivity in the workplace. Employees are much more likely to engage in positive behaviour when they see their employers doing so.
    - Foster Social Connections. Workplace relationships are an essential element to positive company culture. When employees regularly interact with one another, they build a high level of trusts
    - Foster a culture of "champions". Are those employees who embody the values and missions of the organisation. They are excited to promote a company's aspirations and encourage others to do the same. Identify these employees and encourage them to keep spreading the cheer.

## How can we help you?

If you are experiencing accidental data leaks or unintentional actions that have placed your business at risk, then we can certainly help you to sort that out quickly.

To help you identify why your employees are placing your business unintentionally at risk, we need to identify your current "**Employee Trust Engagement " level of maturity**. It's a simple assessment that looks at various areas such as trust, communication, culture, organisation support, job engagement and peer connectivity.

Through a multiple-choice questionnaire, we are able to understand very quickly where your employee trust engagement maturity sits. We are then able to provide you with the right set of recommendations that will help you engender a positive organisation culture.

Interested in conducting an employee trust engagement assessment? Then reach us at insider@commsnet.com.au or https://commsnet.com.au/contact-us

## Contact Us

You can reach us at the following

- Web: www.commsnet.com.au
- Phone: +61 2 6282 5554
- Email: insider@commsnet.com.au
- Twitter: www.twitter.com/commsnetgroup