25% of former employees still have access to data from former workplace

Businesses are putting themselves at increased risk of losing data, by not curbing the actions of current and former employees. Twenty-five percent of workers in South Africa still have access to files and documents from a previous employer, putting the integrity of data and company livelihood at risk, according to new research titled 'Sorting out digital clutter in business' from Kaspersky Lab.

Sergey Martsynkyan, head of B2B Product Marketing at Kaspersky Lab

Former employees can also use this data for their own purposes, for example in a new workplace, or they may accidentally delete or damage it. As a result, data recovery will require time and effort, which otherwise could be spent on more useful business tasks.

With every business today drowning in digital files, using collaboration applications, online documents, and file sharing services, it can be hard for them to keep track of what data resides where, who has access to it, when and how.

However, this lack of clarity when it comes to ‘digital clutter’ is not only an organisational headache: failing to lock down data that lives online could pose a disadvantage or even a threat to business.

Unauthorised access

The risk of unauthorised access to work files may not come from the most obvious party: workers that are no longer with a company but were not cut off from the corporate email service, messenger app or Google documents. The situation is especially worrying as these assets include intellectual property, commercial secrets or other protected or confidential data that, if let loose, could be used by cybercriminals or competitors to their own advantage.

Among the South African respondents that Kaspersky Lab surveyed, 76% admitted working with documents that contain different kinds of sensitive data.

The study also found that due to digital data mess, it takes employees' time to find the right document or data stored in different places. Sixty-two percent of office staff found it difficult to locate a document or file while at work.

Fifty-two percent also use the same device for work and personal use which means that information on different devices can be duplicated or become outdated, causing confusion and possible errors at work.

This digital clutter may also lead to data compromise if it falls into the hands of a third party, or even a competitor. The consequences of this could take the form of penalties and lawsuits with clients, as a result of violation of an NDA or data protection legislation.

The problem of proper access to work assets is also highlighted by the fact that just under a third (28%) of South African workers admit to sharing their username and password credentials for a work device with a co-worker.

A result of an open space culture

In today's office culture of open spaces and collaborative ways of working, employees are often more inclined not to set boundaries but to share everything with their colleagues, from paper clips and ideas to desks, tasks and even devices. Bad password habits and a laissez-faire attitude to sensitive corporate data may seem harmless enough and might not directly lead to a breach, however, it does point towards a need for wider education of the risks.

"Digital files in disarray and uncontrolled access to data can sometimes lead to breaches and cyber-incidents but, in most cases, will likely result in office work disruption, wasted time and lost energy associated with recovering missing files. For businesses - especially small and actively developing companies which strive to be efficient and competitive - the situation is very undesirable. Combating clutter, carefully managing access rights and using cybersecurity solutions is not only about protecting against cyber threats. It is a guarantee of effective work without interruptions, where all files are in the right place and employees can allocate their time to achieving business goals, having all the data they need at hand," says Sergey Martsynkyan, head of B2B Product Marketing at Kaspersky Lab.

Best practices

To make sure digital clutter does not cloud your data security practices, the following steps will help add clarity:

- Set up an **access policy for corporate assets**, including email boxes, shared folders, online documents: all access rights should be cancelled as soon as an employee has left

- Regularly remind staff about the company's **cybersecurity rules**, so that they understand what is expected of them and they become second nature

- **Use encryption** to protect corporate data stored on devices. Backup data to ensure information is safe and retrievable, should the worst happen

- Foster **good password** habits among employees, such as not using personal details or sharing them with anyone in or outside of the company. The Password Manager function in a protection product can help keep passwords secure and your confidential data safe

- If you are used to working with cloud services, you can **choose a cybersecurity solution** from the cloud that fits with your company size