8MAN

# Do you know who's accessing your data?

Results of a survey by Vanson Bourne, sponsored by Protected Networks GmbH

Protected Networks

# Introduction

We live in an age where more devices and technologies are available in the workplace than ever before. We live in an age where high-profile cyber-breaches are reported in our media almost weekly, leaving many of us vulnerable. It stands to reason to assume therefore that we live in an age where companies are paying more and more attention to ensure that they are not embroiled in any data breach scandal. But, while they consider ever-more sophisticated protection technologies, one of the deepest threats actually lies at a more fundamental level. Many organisations are currently leaving themselves at risk by not enforcing strict security procedures when an employee leaves the company. If a former employee is able to retain access to their former employer's network and data, then there are obvious security risks and compliance implications. The former employee and their new employer may benefit, leaving the other organisation at a severe loss. Even if a former employee is highly trusted and contractually bound, it is possible that their out-dated credentials could be more easily stolen than when they were employed, and then used by criminals to gain access to confidential data.

# Key findings

Around half (49%) of IT decision maker ("ITDM") respondents reported that they have retained the necessary rights to access a former employer's network after leaving their employment and a further 17% do not know if they have or not. This suggests that it is actually more likely than not, that any given former employee is allowed to retain their access rights to data after their leaving date. Many organisations are leaving themselves with IT security risks and could be open to losing data or corporate sabotage, among other significant impacts.


Respondents from smaller organisations (1,000-3,000 employees) are more likely to have experienced continued access after leaving (56%), compared to 42% of respondents from larger organisations.

The extent of the rights that are retained can vary. Of interviewed ITDMs who have retained the necessary rights to access a former employer's network after leaving their employment, around two thirds (65%) retained basic network access. This will be giving former employees access to sensitive files and documents that only people still working at the organisation should be able to access. What is even more concerning is that many are still retaining even greater access, with almost a quarter (22%) who report that they retained administrator rights. This is generally perceived as being the highest level of permission that can be granted to a computer user and, as such, this means that the user could have the ability to install software and change configuration settings. This could potentially result in extreme difficulties for those employees who are still legitimately working on the network, as well as for the company itself, whose data is exposed.


In addition, of those who did retain the necessary rights to access a former employer's network after leaving their employment, around three quarters (76%) admit that they did actually make use of these rights and accessed their former employer's

network. Accessing the network once could have been all the employee needed to conduct malicious or accidentally damaging activity. However, perhaps even more worryingly for organisations, more than six in ten (63%) respondents admit that they have made use of their rights more than once.

**76%**

of those **who retained a former employer's network rights did make use of these rights**


*and more than **six in ten** (63%) **did so more than once***

Employers are rarely taking action once network access from a former employee has occurred. Only 16% of those surveyed who did access a former employer's network after leaving, state that their employer was aware they had done so and removed their access as a result. Alarmingly, perhaps, almost three fifths (57%) say that their employer did notice but that they left them with their access. There may be a number of practical explanations for this - but in our modern world where data protection and IT security compliance have become paramount, this finding of the survey should trigger deeply searching questions from all responsible managers and boards of directors. The most worrying question is whether there is a widespread gap, across all industries, between the understanding of top management about detailed IT security practices, and the practical reality as implemented on a day-to-day basis by their heavily overloaded IT administration staff. If there is such a gap, as hinted by the survey, then it is just a question of time until the ever-growing risks materialise.

**Only 16%**

of those **who retained access** to a **former employer's network** said that **their employer realised they accessed the network** and **removed their access**


*while **57% realised but did not have their access removed***

It is not only the right to network access that is a problem; one in ten (10%) ITDM respondents reported that their former employer did not take back hardware that they had been provided for access (e.g. laptop, phone and VPN). This means that any files saved onto that piece of hardware are still accessible to former employees, and ultimately this could be just as costly and dangerous for the security of the organisation.

**10%**

report that their **former employer did not take back** any **hardware** they were **provided for access** (e.g. laptop, phone, VPN)


Most interviewed ITDMs do themselves recognise the need for change in organisations' management of network access rights. Around eight in ten agree that the management of network access rights should be easier (83%) and better monitored (80%). Only slightly fewer (76%) report that the access rights should be given a higher priority and focus of attention. This supports the argument that there is huge value in a solution that can help manage access rights, with efficiency and security. Through improved access rights management, organisations can do a great deal to prevent the scenarios occurring where their former employees can steal or even destroy, their valuable information.

**Atleast 3/4**

agree that **network access rights should be:**

- **easier to manage (83%)**
- **better monitored (80%)**
- **given a higher priority** and **focus of attention (76%)**

## In summary

Organisations are leaving themselves open to deep security risks, compliance violations and large-scale data theft by not restricting their former employees' access to their networks. In the recent past, security breaches and data loss have been the focus of widespread media attention and this should be an area that organisations of all sizes are determined to avoid being associated with.

These concerns should be at the forefront of management thinking, particularly when considering the number of former employees who, according to the survey, are retaining access and actively accessing their former employer's network after leaving.

Management can do a great deal to help prevent these risks by ensuring that an optimal access rights management software solution is in place, which not only provides clarity about existing access rights, but also makes complex changes in the access rights system easy, which logs changes, and which can support improved management processes.

## Methodology

During May 2016, 100 IT decision makers from the UK were interviewed for this piece of research.

To qualify for the research, respondents' organisations had to have at least 1,000 employees, including an even split between organisations with 1,000-3,000 employees and more than 3,000 employees (50 interviews in each size band). Organisations could have been from any commercial sector, but with particular focus on the following sectors:

- Business and professional services
- Financial services
- IT
- Retail, distribution and transport
- Manufacturing

IT decision makers were interviewed using an online methodology and a robust multi-level screening process was used to ensure that only appropriate respondents participated in the project.

## About 8MAN

The 8MAN solution scans and displays the data access rights structure within an organisation in a clear, graphical and simple manner. It shows you immediately who has access to a resource, how they have access, and allows changes with a few clicks. Security gaps can be quickly identified and closed. Changes can be carried out using 8MAN, following best practice and policy guidelines – saving considerable time and resources.

8MAN also has a wide range of audit reports and activity logs which will speed up compliance projects. 8MAN saves time and reduces costs while also closing dangerous security gaps in data and user management.