The Insider Threat Security Manifesto / BEATING THE THREAT FROM WITHIN

IS Decisions

EXECUTIVE SUMMARY

Ask any IT professional to name the security threats to their organisation and they will probably reel off a list of external sources; hackers, viruses, denial of service attacks and phishing.

But are these dangers from outside of a business really the greatest security threat?

More often than not the greatest risk to any organisation comes from within. That unhappy employee, or rogue insider who will go to any length to gain access to the organisation's crown jewels, share the sensitive data they get their hands on and even put it to some other **unscrupulous use** such as insider trading.

As the Edward Snowden scandal highlighted, if a disgruntled worker is determined to unearth critical information, it is not that hard to do so. Snowden was an IT contractor, but he gained access to files he should not have by simply asking his colleagues to **share their passwords**. Once he had the log on details, off he went in search of highly confidential and sensitive data.

Of course, malicious employees are the exception rather than the rule. But they are not the only insider threat. **Ignorant users** are also perilous, and Forrester research has shown that the greatest volume of security breaches (36%) come from employees inadvertently misusing data. They unwittingly share sensitive data or information that could fall into the wrong hands almost daily. And of course, many employees casually share passwords. Giving their ID to who ever asks for it as an apparent necessity or just to make their lives easier, without any idea of why it might cause a security breach.

"The day-to-day internal security threat faced by most organisations is not due to malicious behaviour; the 'insider threat' is most likely to be down to the misuse and poor use of IT. This in turn is often caused by inadequate policies and practices in the first place. A good example is the sharing of usernames and passwords, which exacerbates the problem because issues arising cannot be associated with individual users. Many aspects of the insider threat can be mitigated with **investment in tools** that monitor and, to a certain extent, control users, for their own benefit and for that of the organisation they work for."

Bob Tarzey
Analyst and Director, Quocirca

To find out how organisations are attacking insider threats we conducted a study of 500 IT decision makers in organisations ranging from 50 – 10,000 people in the UK and US (250 in each respective country) to understand what their attitudes are to the threat from within and how they are approaching it.

Drawing on the results of the research, this security manifesto will **empower IT professionals** to take proactive measures to help them beat the threat from within. While no system is ever going to 100% stop the problem, with the appropriate steps the risk can be significantly diminished.

CONTENTS

KEY FINDINGS

35% of organisations with over 10,000 employees in the UK and US have suffered an internal security breach in the past 12 months

12% of IT professionals are more aware of insider threats as a result of the Snowden scandal

19% IT professionals estimate an average of 19% users are sharing passwords

44% told us that data loss is their greatest concern, placing it higher than insider threats, despite employee behaviour being the greatest source of data loss

Insider threats are not IT professionals'
TOP SECURITY PRIORITY
lagging behind viruses, data loss and hacking

IGNORANT USERS
cause the greatest internal security concern

There is **SOME CONFUSION**
about what network management capabilities IT professionals have to prevent insider threats

Many IT professionals are not sure if they are compliant with
INDUSTRY REGULATIONS
with specific requirements around insider threats

WHERE INSIDER THREATS SIT ON THE IT SECURITY AGENDA

How concerned are IT professionals about insider threats? Are the common assumptions about security threats being a primarily external concern the same for those whose job it is to mitigate these risks?

In short, yes.

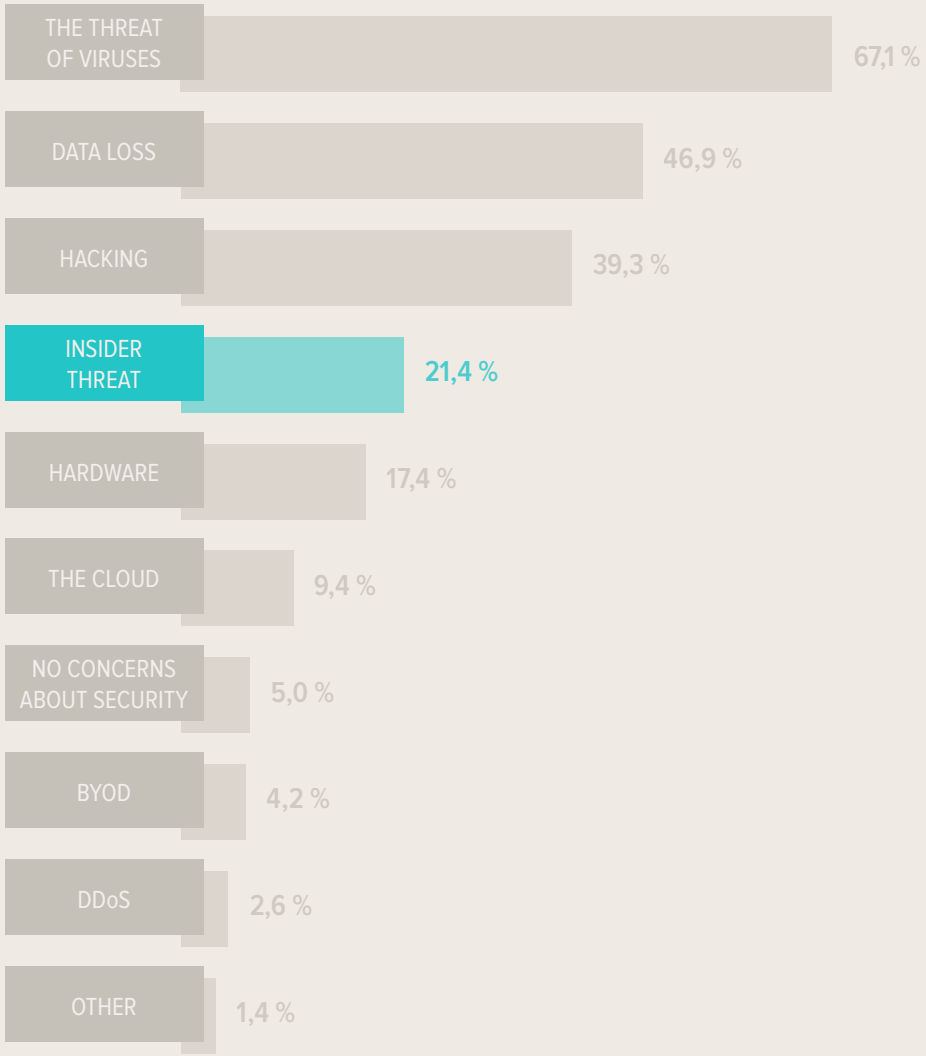
When asking IT decision makers across the UK and US to list their three greatest security concerns, we found that insider threats comes fourth on the list with **only 21% putting it in their top three**, behind viruses (67%), data loss (47%) and hacking (40%).

So insider threats, including password sharing or employees accessing sensitive information, appears not to be a great concern to the majority of IT decision makers.

There is a point to be made here however, in that data loss is a concern for more than twice the amount that insider threats are, and as we know employees are the most likely cause of data loss.

So why aren't IT professionals more concerned about this risk?

WHICH AREA OF YOUR IT CAUSES YOU THE GREATEST SECURITY CONCERN?



Who is more concerned about insider threats?

Comparing the two geographical areas we looked at, it seems that IT professionals in the UK are more concerned about internal security risks than their US counterparts. We found that 21% in the UK listed insider threats in their top three concerns, but only 17.5% in the US.

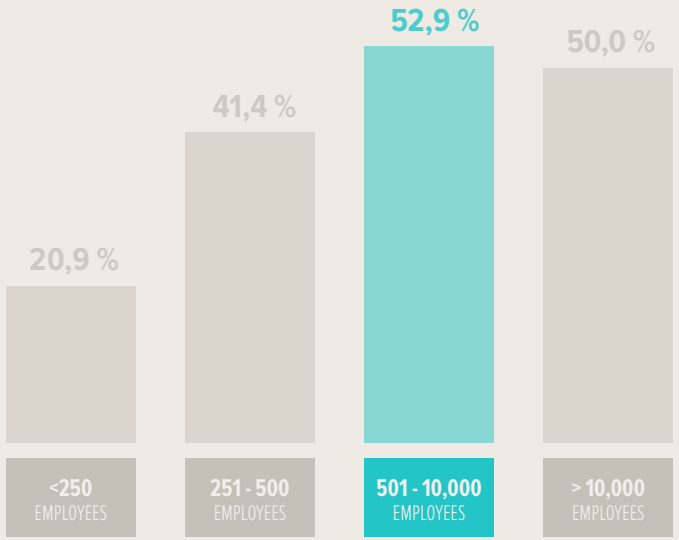
It also tends to fit, in both the US and the UK, that **the larger the organisation, the more of a concern it is**, with 52% of IT managers in organisations of 501 – 10,000 employees. This drops slightly to 50% for those above 10,000, potentially as these larger organisations have stronger internal security policies.

This is a natural trend of course, as the more employees your organisation has the greater the statistical likelihood is that you may have some that are unhappy, and the harder it is to **manage issues** such as password sharing.

MANIFESTO

Implement a 360-degree security policy that addresses both internal and external threats, and be transparent about what risks your policy is mitigating

PERCENTAGE OF IT PROFESSIONALS LISTING 'INSIDER THREATS' IN THEIR TOP THREE SECURITY CONCERNS



THE EDWARD SNOWDEN EFFECT: IS AWARENESS OF INSIDER THREATS GROWING?

We've mentioned that Edward Snowden's actions last year put insider threats on the media agenda, but how has that translated into the consciousness of IT professionals?

We asked whether IT professionals worry more about insider threats more now than they did 12 months ago, and 19% said that they did. More specifically, 12% said that they are **more aware since the Edward Snowden scandal**.

Interestingly, this number was marginally higher in the UK, where the story was broken, than the US where it actually took place, with 13% of UK IT professionals agreeing and 11% in the US.

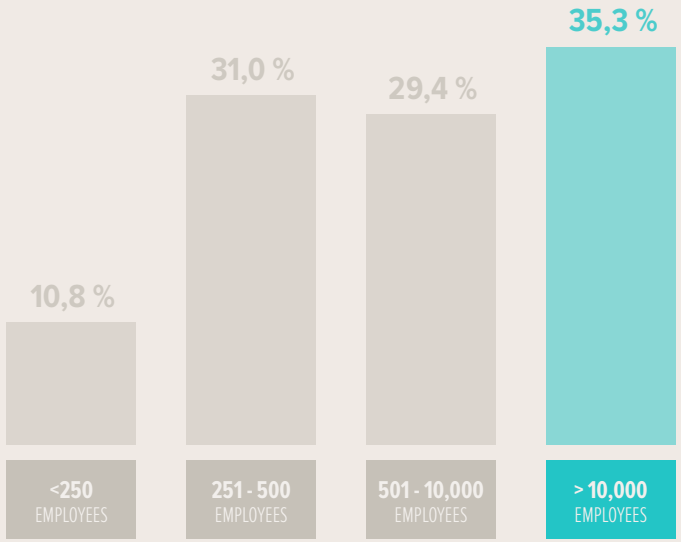
Again, it is within larger organisations that the concern about insider threats has grown most. 38% of IT professionals in organisations of over 250 employees told us they have become **more concerned in the last 12 months**, compared to 17% for those of 250 and under.

Our assumption that risk of the occurrence of insider threats is greater within larger organisations was also borne out in asking where internal security breaches have actually occurred in the last year.

On average, 12% of organisations told us they had suffered an internal security breach in the last year. This number was higher in the UK at 14%, compared to 9% in the US. Given there were 2.17 million businesses registered in the UK in 2013, this suggests that there were over **300,000 internal security breaches** in the UK last year. Of the 7.4 million businesses with employees in the US, this translates to at least **666,000 occurrences of internal security breach**.

So this may constitute some of the 19% of IT decision makers that told us they have become more worried about insider threats in the last 12 months; naturally you would be more concerned about a security issue once you have experienced it.

MY ORGANISATION HAS HAD AN INTERNAL SECURITY BREACH(ES) IN THE PAST YEAR



There is another caveat here in that awareness of all security threats are growing. We also asked whether worry about external security threats had grown over the last three years, with which 46% agreed. This highlights again the fact that organisations are **more concerned** about external threats than internal.

However, the fact that more than one in ten IT professionals told us they were more aware of the dangers of internal threats as a consequence of the scandal shows that Edward Snowden has inadvertently shone a light on what is a significant security issue for IT professionals.

Insider threats continue to be an under-addressed problem

Still not significant enough for many though, it seems. It is concerning that despite most security breaches coming from employees, and the greater awareness Snowden has created of insider threats, as a security concern for IT decision makers it is still a **laggard** behind viruses and hackers. It is odd that IT professionals list data loss as a greater concern ahead of insider threats, when we know that employees are the greatest cause of data loss.

When asking IT managers to score their overall security policies out of 10, larger businesses were more confident with the score being 8.29 for those with more than 10,000 employees, compared to 7.23 for businesses of all sizes. This is interesting considering the considerably greater number of occurrences of internal security breaches in larger businesses, reiterating the suggestion that IT managers are **not considering insider threats seriously enough** in their overall security policies.

MANIFESTO

Ensure your policy is clearly documented and accessible, consistently remind users of its stipulations

PASSWORD SHARING AND WHERE THE THREAT LIES

We have highlighted that password sharing is a key area of concern with regards to insider threats. But what kind of users are IT managers concerned about within their organisations? **How prolific** do they believe password sharing to be and how do they think it occurs?

In terms of security risk, IT professionals are far more concerned about **ignorant users** than any other group. 42% told us they considered them to be the greatest security risk in their organisation, ahead of tech savvy users who may be attempting to get around internal security protocols, or external visitors such as clients, customers and suppliers.

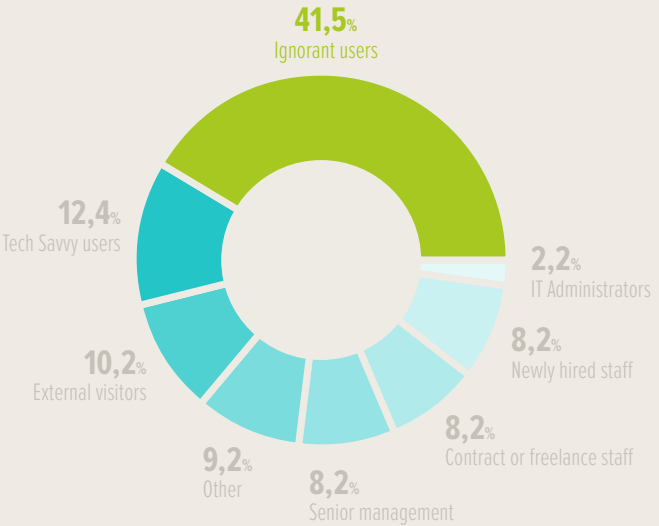
IT managers concerns here are not misdirected, ignorant users are **a great security risk**. Those that are not aware of the dangers of sharing passwords or other sensitive information are most likely to pass it on to malicious users.

We also see senior management is considered to be of as great a risk as new hires or contract staff. All of these groups could include ignorant users, but you would expect senior staff to be less so in comparison to new or temporary employees. However, it is often the case that senior management are **the worst culprits** for password sharing, as they are the most likely to do so in order to delegate work, and many work under the assumption that the rules do not apply to them.

MANIFESTO

Combat password sharing by restricting concurrent logins

IN YOUR OPINION, WHICH GROUP WITHIN YOUR ORGANISATION REPRESENTS THE GREATEST SECURITY RISK?



How prolific is password sharing?

We asked IT professionals what percentage of people they believe are sharing passwords within their organisation. Across all organisations and industries, the mean average was 19%, a number that did not differ between the UK and the US. This means that if IT's estimates are correct, just under **one in five people** are sharing their passwords with colleagues.

However, the greatest volume of IT professionals (35%) told us that **they believe no one is sharing passwords** in their organisation.

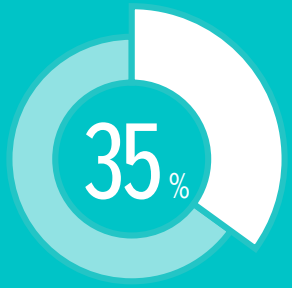
Great news, if true. Looking at this information in isolation it is possible to assume that over a third of organisations have all the necessary precautions in place to prevent password sharing, or just have a completely compliant and educated workforce.

Realistically though, this is unlikely, leading us to conclude that there is some **naivety or lack of education** even among IT professionals about the proliferation of password sharing.

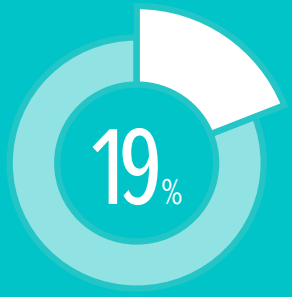
MANIFESTO

Combat password sharing by limiting users to workstations, locations, devices, user groups or departments

HOW PROFILIC IS PASSWORD SHARING?



of organisations believe no one is sharing passwords



of users share their password in an organization

What type of organisation is most likely to have a culture of password sharing?

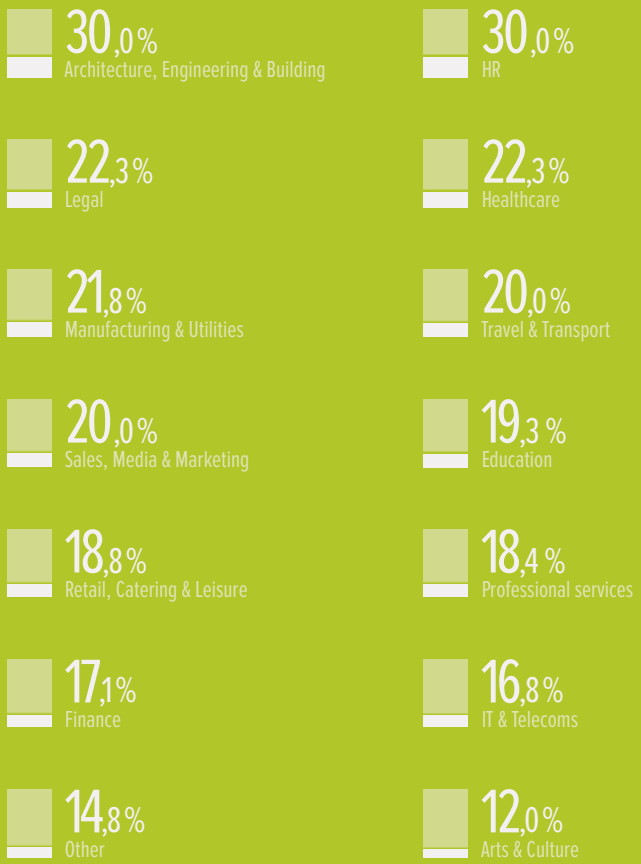
Splitting the results across different sectors reveals that architecture and HR are the industries where password sharing is most prevalent, or at least the industries where IT is most aware of it, with the **mean average estimate** in the industries being **30%**.

One industry with a surprisingly high placement on the list is legal (mean average 22%), where a lot of sensitive information is handled and regulations are strict. Is it possible that the restrictions in place in order to ensure regulatory compliance are contributory to the cause of employees sharing their passwords?

Looking at how the numbers differ across organisation size helps to explain why such a **high proportion** do not believe there is any password sharing present in their organisation. IT professionals in organisations with under 50 employees were far more likely to answer this way, with 45% saying no one shares passwords in their organisation. To be expected, given the fewer employees you have the less necessity there is to share information across departments and again the easier it is to manage.

Removing organisations of under 50 employees, 0% ceases to be the most popular answer, with 40% answering 10% and the mean average increasing to 23%.

PROPORTION OF USER PASSWORD SHARING PER SECTOR



When do users share passwords?

We also asked when IT professionals believe their users are most likely to share passwords. The most popular answer (given by 25%) was, quite simply, when a **colleague asks for it**.

This highlights that the problem of password sharing is more than a technology issue; it is a behavioural issue. If 25% of UK and US office workers just need to be asked by a colleague to give up their password, anyone wishing to use social engineering to gain network access they should not have will not have to try very hard.

Just behind this answer, stated by 24.6%, was **'when delegating work'**. This links to the issues raised earlier of users believing password sharing is necessary, and senior staff giving out their passwords in order to delegate.

The conservative average estimate of just under a fifth of employees **sharing passwords is a significant problem**, and one that you would expect IT professionals to want to address. Understanding why people share passwords is a key part of doing that, as we've highlighted it is a behavioural issue as well as a technology issue that must be approached from both sides. That means educating people about the dangers of password sharing, but using technology to help people adhere to the policies too, as there will always be people who will try to break the rules.

MANIFESTO

Limit network access to working hours or specific session times to help ensure the logged in user is who they say they are

ACTIVE DIRECTORY AND INSIDER THREATS

Having identified that password sharing is a gateway to internal threats, a great security risk that is rampant in UK and US organisations, what are IT professionals doing to attempt to tackle the issue?

Microsoft Active Directory's internal security loopholes

Active Directory (AD) is the directory service included with most Windows Server operating systems, for Windows domain networks. In a Windows environment, an AD domain controller authenticates and authorises all user and computer logins.

It is very widely used; our research found that AD is used by 87% of organisations over 50 employees in size. Unfortunately, **AD is not particularly well set up to tackle insider threats or password sharing.**

It lacks the ability to do any of the following –

- **Limit or prevent concurrent logins:** Users are far less likely to share their network password if they know they cannot get access while another user is using it.
- **Manage access restrictions:** Using AD in isolation it is practically very difficult for the administrator to set rules and restrictions around when and how users access the network.
- **Real time monitoring:** It is also virtually impossible to get a clear picture of the who, when and where of user network access.

Ultimately, using AD alone, even if IT administrators have a security policy to try and combat insider threats, it is likely to be difficult to enforce.

"Active Directory provides basic user security, checking that credentials supplied match stored user profiles and then opening up access to resources. Authenticating those credentials is another matter; for this organisations need to turn to **stronger authentication techniques** to ensure a user really is who they say they" are.

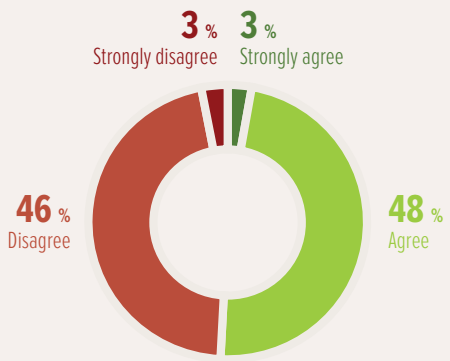
Bob Tarzey
Analyst and Director, Quocirca

Active Directory users' security awareness

How aware are the IT professionals using AD of its security loopholes?

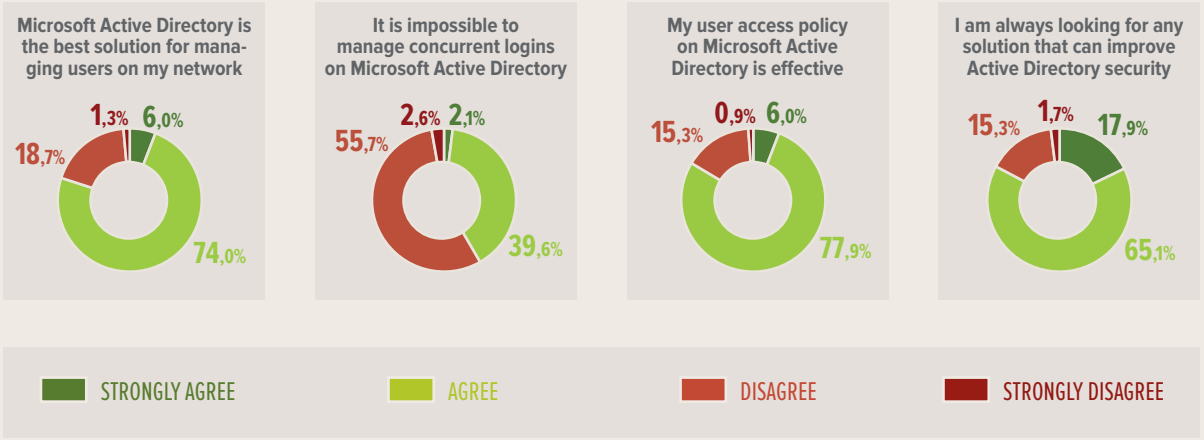
We asked the IT decision makers that had told us their organisation is using AD if they strongly agreed, agreed, disagreed or strongly disagreed with a number of statements.

There are no security holes in Microsoft Active Directory



The first was the statement 'there are no security holes in Microsoft Active Directory', with which the marginal majority (51%) agreed.

We then asked the following –



We can see here that clearly, AD is popular with its users; they overwhelmingly believe that it is the best solution for managing their networks.

However, they seem to be split on the topic of its security strengths. It's concerning that the majority are unaware of any **security loopholes**, but more worrying that an even larger majority (69%) believe it is possible to manage concurrent logins in AD. Although it is technically possible to view concurrent logins, using custom scripts, it is **not possible** to limit or prevent them in a secure or effective manor.

We then see that nearly 9 in 10 (84%) believe that their user access policy is effective.

This leads us to believe that even among the 49% who acknowledged AD may have security loopholes, many **don't know what those loopholes might be**.

The good news however, is that despite the fact that 84% told us their AD user access policy is effective, a similar figure of 83% are always on the look out for a solution that can **improve AD's security**.

Network management capabilities

Looking at the more specific details of what IT professionals are able to do with regards to network management, we made some interesting findings. On average, the majority (70%) of IT professionals believe that their network management solution allows them to **manage concurrent users**. This is the case even for larger organisations, which we know overwhelmingly use Active Directory, with which it is not possible.

This trend was repeated for other capabilities, such as setting session time outs and monitoring sessions in real-time. This begs the question of how accurate IT professionals' own perception of their network management ability is, given we know that the majority of large organisations are using Active Directory, on which these **granular levels of user access control are not possible** or at least very difficult to deploy.
This tallies with the fact that the majority of IT professionals are either unaware of Active Directory's security loopholes, or if they are aware they don't know what those loopholes are.

MANIFESTO

Active Directory provides basic security, but it is important to build on that with real time monitoring and further restrictions to what users can do once authenticated

WHAT DOES YOUR CURRENT NETWORK MANAGEMENT SOLUTION ALLOW YOU TO DO?

	< 50 EMPLOYEES	51 - 250 EMPLOYEES	251 - 500 EMPLOYEES	501 - 10,000 EMPLOYEES	10,000 + EMPLOYEES
Manage concurrent users	64%	73%	86%	88%	91%
Prevent logins on multiple workstations	48%	67%	52%	53%	68%
Define specific times for user access per person	29%	60%	48%	51%	62%
Define specific times for user access per group	24%	57%	52%	47%	56%
Set 'sessions' so users are timed out	38%	70%	72%	75%	82%
Monitor real-time sessions	38%	63%	69%	75%	82%

NETWORK MANAGEMENT AND COMPLIANCE

In addition to the considerable motive most organisations have to address insider threats themselves, many work under industry regulations that either directly specify how it should be addressed, or are closely related to the issue.

Examples of these include:

Sarbanes-Oxley (SOX)

The US Senate's 2002 act is federal law relating to standards for public company boards and accounting firms. It closely relates to insider threats in its strict terms around the reporting it requires, and how unauthorised users must not be able to modify these reports, as well as granular requirements for internal controls of financial reports.

Payment Card Industry Data Security Standard (PCI DSS)

A set of requirements laid out by the PCI Security Standards Council, which is made up of the world's main payment card brands, PCI DSS applies to any business taking card payments. It relates to the protection of cardholder data, and has specific IT security requirements for firewalls around that data, password protection, network access restriction at a user-level as well as access tracking and monitoring.

Health Insurance Portability and Accountability Act (HIPAA)

Another US regulation, HIPAA relates to health insurance and the privacy and security of health data.

Federal Information Security Management Act (FISMA)

FISMA has very specific requirements around the security of inventory information, as well as categorising, security control and continuous monitoring, for any federal agencies in the US.

We've revealed that many IT professionals seem to be confused about what their network management solution enables them to do in terms of **user restrictions and monitoring**. However, presumably when working in an industry that is subject to legal regulations, IT pros are more aware of whether they are compliant.

SOX Compliance

Only 50% of IT decision makers in US finance sector organisations told us they were SOX compliant. Among those in organisations of over 10,000 (and therefore more likely to be publicly listed), 78% told us they were compliant.

HIPAA Compliance

IT professionals in the US health care industry appear to be stricter with regards to regulatory adherence, as 82% told us they were HIPAA compliant. However this did still leave 7% who said they were not, and 11% who didn't know.

PCI DSS Compliance

Most businesses make card payment transactions, but the sectors where these tend to be high volume and PCI compliance is more important are naturally retail and finance. However, only 27% of IT professionals in retail businesses across the UK and the US told us they were PCI compliant, with 50% saying they didn't know if they were or not. Finance was even worse, with 52% saying they didn't know, and only 19% stating they were compliant.

Know your regulatory requirements

The key outtake here is that generally, IT professionals are not as aware of the regulatory requirements that their industry is under as they perhaps should be. These regulations require IT decision makers to understand and address them, as **technology is often central** to ensuring they are met.

MANIFESTO

Make regulatory requirements a part of your security policy

TEN STEPS TO BEATING INSIDER THREATS

We've established that insider threats are a **serious security concern**, one that needs to be higher up on IT professionals' agendas. However, mitigating the risks is not a simple task.

Nearly 9 out of 10 (86%) of IT professionals told us they did not realise that technology could help solve insider threats, so they seem to understand it as more of a cultural and organisational issue. Which it is, but technology can certainly help **mitigate the risks**; an optimum strategy should approach the issue from both angles.
This is our manifesto for beating the threat from within.

LIMIT OR PREVENT CONCURRENT LOGINS

1.

In technology terms, this is your **first line of defence** against password sharing. If users know that giving their password to a colleague means their own network access will be restricted, they will be much less likely to do it. What's more is that in the event that a rogue user does gain valid credentials that they shouldn't have, they will be prevented from using them at the same time as the legitimate owner. This means that **access to critical assets** can be more authoritatively attributed to individual employees, helping to affirm accountability and avoid repudiation issues when there is an internal breach.

LIMIT WORKING HOURS OR MAXIMUM SESSION TIME

Someone looking to gain access to files that they shouldn't have is likely to do so outside of normal working hours, in order to **lessen the risk of being caught**. While network access attributed to a user inside of their set working hours is more easily identifiable to that individual.

2.

LIMIT USERS TO THEIR OWN WORKSTATION OR DEPARTMENT

3.

By limiting users to specific workstations, devices, departments or IP ranges you are effectively **reducing the network surface area** that is open to any kind of attack. In reducing the number of computers or devices on which a compromised user's credentials can be used, you are reducing risk.

MONITOR USER BEHAVIOUR IN REAL TIME

Once restrictions such as these are in place, monitoring user access should be made easier. Tracking and reporting is only so useful when done in retrospect, so ensure you are monitoring in real time in order to **recognise suspicious activity** when you are able to respond.

4.

RECOGNISE AND RESPOND TO SUSPICIOUS BEHAVIOUR

5.

And do respond when you spot suspicious activity. **An immediate response** should be an integral part of an organisations security policy and risk mitigation strategy. By responding quickly, even if the threat is a false alarm, showing that action is taken swiftly helps to **educate users and reduces the risk** of malicious insider activity.

DEACTIVATE COMPUTER ACCESS FOLLOWING TERMINATION

Former employees are another kind of internal threat, and often are left with their network access open following the termination of employment, when they may be more motivated to access sensitive information. It is crucial that you ensure their accounts are **closed swiftly** following termination.

6.

IMPLEMENT A SECURITY POLICY

7.

It is great to have technical limitations on passwords and network access, but ensure you have a written policy too. 29% of the IT professionals we surveyed told us they don't have a security policy at all, which is very worrying. Make sure you have one, and make sure **it explains why as well as what** your policy is. Be transparent about the risks your policy addresses and if you are in an industry that is subject to regulations then explain in understandable terms what those regulations are and why they're important.

CLEARLY DOCUMENT POLICIES

Security policies should be clear, accessible to everyone and understood by all in your organisation. 41% of IT professionals said their security policy was included in an employee handbook or manual.

8.

CONSISTENTLY REMIND USERS OF POLICY

9.

Including a security policy in a company handbook, located somewhere accessible to all, is great but it is **just the first step** to ensuring users understand it. We all know that these can get read in an employee's first week on the job, and then forgotten about. There is also a chance that users who are consistently trying to gain network access outside of restrictions will get frustrated. Remind them why the restrictions are in place, and what they can do instead to get the job they need to do done, like ask for temporary clearance.

Mentioning contractual or legal implications here also helps highlight the **severity of the issue** to the user. Technology can help here too; we found that just 12% of the IT professionals we surveyed remind users of security policies with **daily prompts**. With some security applications it is possible to set up customisable alerts and prompts to ensure users are reminded of security policies in an effective way.

WORK CLOSELY WITH HR AND OTHER DEPARTMENTS

10.

We have explained that mitigating insider threats is not just a technological problem. IT is responsible for managing network access, but not generally for managing sensitive employee information; that tends to be the remit of HR. Working closely with other departments may help with **educating users** on your security policy, HR could include it in the training schedule for instance.

It also may **help in identifying potential internal threats**, as HR are much more likely to be aware of issues where employees may be disgruntled, as well as having a closer track on new starters and employee terminations.

CONCLUSION

Considering that there were an estimated 300,000 internal breaches of security in UK organisations last year, and more than twice that in the US, it is surprising that insider threats are not further up the IT agenda. Perhaps the lack of awareness of how technology can help holds IT professionals back from attempting to tackle it.

What is good, however, is that awareness does seem to be increasing. Our research findings here echo our own experience when talking to those in the industry. IT professionals are becoming more security conscious, and internal security is becoming a bigger part of that.

With the approach we've laid out here, IT professionals that are looking to mitigate the risks of insider threats will be better equipped to do so.

About IS Decisions

IS Decisions makes it easy to safeguard and secure your Microsoft Windows and Active Directory infrastructure. Over 3,000 customers around the world rely on IS Decisions to prevent security breaches; ensure compliance with major regulations, such as SOX, FISMA and HIPAA; quickly respond to IT emergencies; and gain time and cost-savings for IT.

www.isdecisions.com