Staff migration: The Security Impact to Businesses

ilex International

www.ilex-international.com

The risks associated with job migration

Research shows that over half (59 percent) of the UK workforce is actively looking for a new job in 2016*. This is due to the improving economy, with employment rates at their highest in years and an overall increase in wages. This high level of movement amongst the UK workforce could mean serious security implications for businesses.

Businesses urged to strengthen security

With this in mind, Ilex International is reminding businesses of the importance of controlling access to IT systems and sensitive data, especially when employees or contractors leave the company. If a person's account is left open once they have left the company, this becomes an easy access route for cyber criminals. Closing these accounts quickly is a crucial step businesses must take in order to reduce the risk of an attack.

Research carried out by Ilex found that 39 percent of large businesses took up to a month to close dormant accounts, leaving the door open to opportunistic hackers and disgruntled former employees. However, large businesses performed better than small and medium size businesses, with 58 percent removing access to data on or before the day of departure, compared to 56 percent of medium and 32 percent of small businesses.

As the number of security breaches resulting from insider threats increases, security should be front of mind for any organisation seeing changes in staffing in 2016. Ilex' Breach Confidence Index found that 44 percent of IT decision makers from large businesses identified insider threats as the reason for previous security breaches. Whether or not the attack is carried out by a current or past employee, it's imperative that a solid identity and access management solution is in place to prevent sensitive data getting into the wrong hands.

"Businesses must come to terms with the reality of cyberattacks, focusing on 'when' they will happen, rather than 'if' they will", said Thierry Bettini, Director of International Strategy at Ilex International. "The UK is one of the leading economic centres in the world, making it a major target for cyberattacks. Combined with the expected staff migration this year, businesses are facing increased risk and should ensure strict security controls are in place for employees. Shutting down dormant accounts quickly is a simple way for businesses to protect themselves."

IT departments will be hit hard

With UK unemployment at a ten year low at the start of 2016, the economy is looking healthier than we have seen it in recent years. Research shows that 71 percent of IT employers will be increasing pay in 2016**, however much of the workforce still feel underappreciated and underpaid.

Three in five IT professionals will be looking for new jobs in 2016**, raising further alarm for UK businesses. The mass exodus in this department is likely to increase the security risks due to the lack of continuity in the IT security team, combined with the knowledge of the individual employees on the team.

“As the economy picks up, we’re expecting big changes in the workforce this year. The IT sector alone is expected to see sixty-three percent of UK professionals looking to change jobs in 2016[1]”, said Simon Hember, Group Business Development Director at Acumin Consulting. “The movement in this department could result in increased security implications, with those responsible for controlling access to systems also in transition.”

Best practices for controlling account access and minimising the security risk of a shifting workforce

In order to minimise the risk of account access from unwanted persons and the inherent risk to sensitive data, Ilex International recommends five best:

1. **Shut down inactive accounts**
   As employees and contractors constantly change jobs and move around, businesses must make sure they quickly close down inactive accounts. The access associated to these accounts also needs to be removed promptly, eliminating another possible entry point for cyber criminals.

2. **Focus on protecting critical data**
   When it comes to security, there is no such thing as zero risk so it’s key for businesses to focus on protecting critical data. By being aware of what the most sensitive data is, companies can ensure it is available only on a need-to-know basis.

3. **Track and audit data**
   Access to data should be closely tracked and audited to ensure only users who are meant to access critical data have permission to do so. By having the IT department carefully audit sensitive information, companies can feel more confident that their information is only being accessed by those that have permission to do so, with processes in place if any anomalies do occur.

[1] Hays UK Salary and Recruiting Trends 2016: http://www.hays.co.uk/salary-guide/index.htm

2 Hays UK Salary and Recruiting Trends 2016: http://www.hays.co.uk/press-releases/it-sector-enjoys-large-salary-increases-in-2015---but-war-for-talent-to-intensify-pressure-on-employers-1532646

4. **Implement a strong Identity and Access Management solution**
   Identity and Access Management is the foundation of a secure system and enables companies to manage their users and know who is accessing their data. By having this in place, organisations are preventing cybercriminals from accessing corporate systems, rather than finding a way to get them out once it's too late.

5. **Educate employees**
   Companies can also minimise risks by educating employees on the importance of cyber security and the impact a breach can have. Lack of employee education was cited as a key reason for security breaches by 15 percent of respondents in the Breach Confidence Index. With the workforce constantly shifting, this has to be done on a regular basis in order to be efficient.

Methodology

Ilex International commissioned YouGov Plc to conduce the Breach Confidence Index survey among British IT decision makers across small, medium and large businesses from 6th-12th August 2015. The survey was carried out online with a total sample size of 530 IT decision makers.

For more information on Identity and Access Management solutions, visit:
www.ilex-international.com/en/

About Ilex International

Ilex International is a European Identity & Access Management (IAM) software vendor. Founded in 1989 Ilex offers a comprehensive solution including identity management (identity, rights and role management) and access management (authentication, access control, SSO, identity federation and card management). The company invests heavily in R&D, providing state of the art technology and services to a large international customer base across finance, defence, healthcare, government and retail sectors.

For more information: www.ilex-international.com/en/

Ilex International Headquarters

✉ contact@ilex-international.com
🌐 www.ilex-international.com

International offices

- London
- Paris
- Marseille
- Rabat