itlab

How to Protect Sensitive Recruitment Data:

with User-Friendly Technologies and Trusted Services

Contents

Introduction

In the recruitment industry, your data and relationships are the bedrock of your success. If your sensitive information were to be lost, stolen or leaked, the financial consequences could be severe. Your reputation could be harmed, driving clients and candidates to your competitors.

Equally, any operational downtime recovering from a data breach could be crippling. A robust strategy to keep your data safe and out of the wrong hands is crucial. Fundamentally, the best controls are those which:

> Are appropriate; your security measures should be balanced with your risk appetite.

> Are straightforward to implement and manage.

> Fit how your business operates and how your users work.

> Reduce the likelihood of a data breach.

> Contain and minimise the consequences of a successful breach.

> Don't frustrate or hinder your user-base.

> Aid compliance with important regulations, such as GDPR.

> Are scalable and cost-effective.

At IT Lab, we support many global recruitment agencies and consultancies. We've come to know your needs and challenges well. In this guide, we introduce and explain some of the most relevant technologies for your sector.

Our clients, including Phaidon International and Heads! Executive Consultancy, are benefitting from these technologies now. They tell us they enjoy peace of mind and have more time to focus on their core activities, such as billing.

We hope you find the following advice helpful and would be delighted to have the opportunity to assist you too.

Michael Bateman
Director of Cyber and Managed Services

Identity and Access Management

	Users	Devices	Apps
Old World	Compliant users working from the office.	IT owned and managed endpoints.	Business systems in data centres protected by firewalls.
New World	Empowered users and remote workers demanding agility.	Diverse set of devices: BYOD, mobile, PCs.	Agile, cloud based apps with no perimeter.

In this new world of cloud computing, people are working differently. The ability to work remotely and login from any device, anytime, anywhere, helps them to be more effective.

But this freedom brings challenges. How can you be sure that only the right people are accessing your systems? If you allow staff to use their own devices, what if they're sloppy with critical security updates?

And what about when people leave? Your sector is known for its high turnover. Leavers may feel a sense of entitlement over information they've helped to build, unaware it's a criminal offence to take it with them.

Clearly it's vital that ex-employees can no longer access sensitive data. Changing passwords each time someone leaves can be onerous, and there's always the risk that some applications could be overlooked.

Without good visibility and security, your data could be needlessly exposed. Identity and Access Management (IAM) addresses the risks elegantly. It can be helpful to think of IAM as a coin: one side bolsters security and the other side benefits your user base.

IAM enables you to control who has access to your systems - and how they do it. This is called authentication. Two-factor authentication (2FA) or multi-factor authentication (MFA) requires the user to verify their identity before access is authorised.

Two-factor or multi-factor authentication applies two or more methods to verify an individual's identity. This is typically something that they know and something that they have e.g. answering a security question and scanning a fingerprint.

All devices are catalogued on a dashboard, placing the power with your IT team to grant, deny and revoke access to both on-premise and cloud applications. The dashboard also provides a variety of useful insights.

Dashboard › Device Insight

Device Insight

Reports

Devices

14 Devices
are Out-of-Date
Edit your policy
to block these devices

18 Devices

78% - out of date

22% - up to date

4 Devices
are Up to Date

Types of Devices

- **33%** Laptops & Desktops
- **67%** Mobile Devices

Trusted Endpoints

- **0** Trusted Endpoints
- **67%** Not Trusted Endpoints
- **12%** Unknown

With IAM, revoking access for leavers is easy because there can be one point of disablement. Setting up new starters is potentially simpler too.

“I want to work with somebody that’s able to provide me with advice and recommendations but also gets the business – understands the strategy that we’re looking to deliver and the way in which technology plays such an important part to underpin the business.

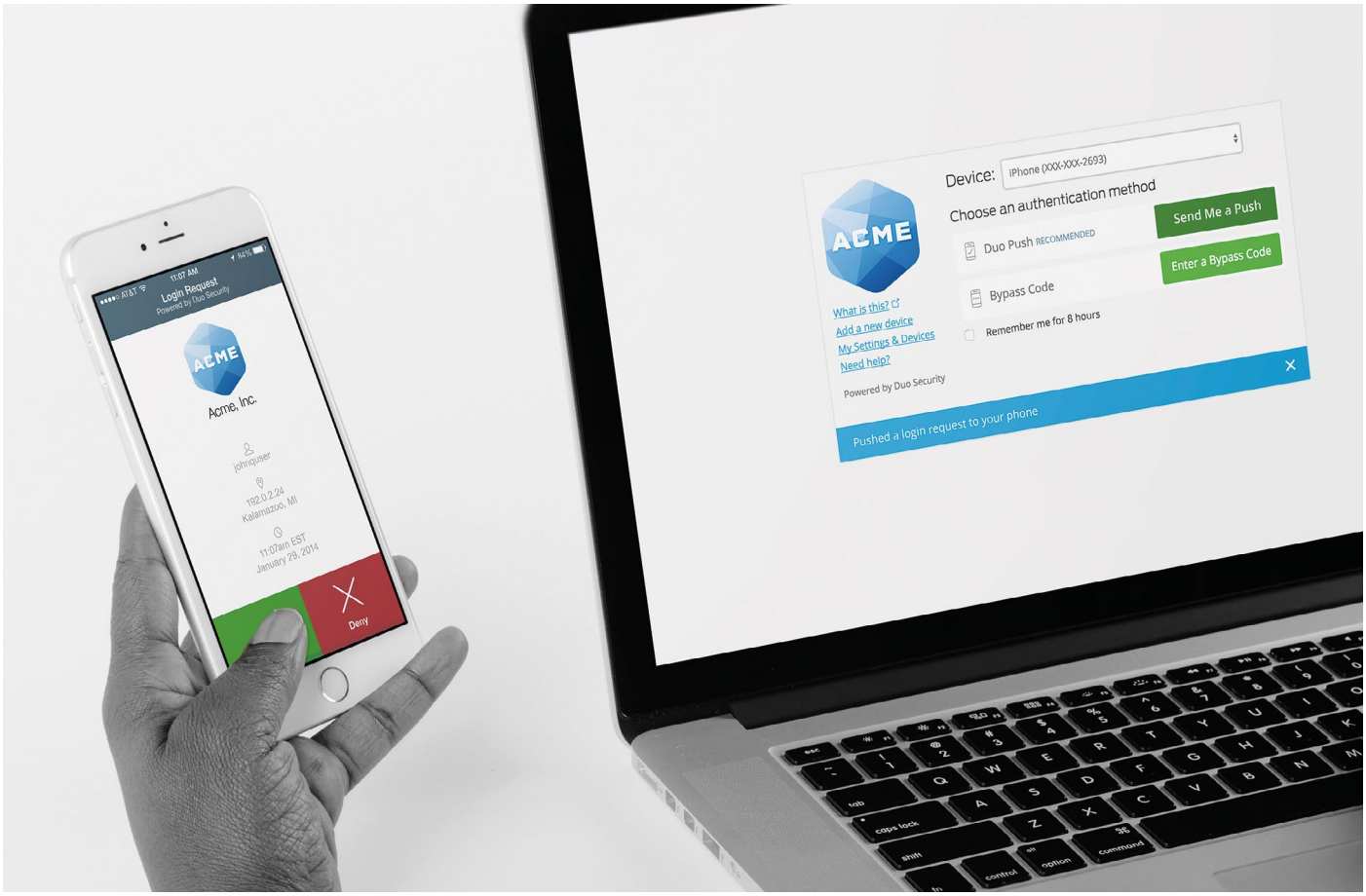
User experience is paramount. IT Lab understand that if we have a poor user-experience, our guys can’t operate in the way that they need to. If they’re not operating optimally, they’re not making money.”

Stuart Pepper, CIO - Phaidon International

Single Sign-on

The other side of the Identity and Access Management coin is Single Sign-on (SSO), which is about making the user experience positive and efficient. How? By giving your users one set of credentials and a single point of entry to your cloud systems.

This means they’re not required to login to your systems individually or memorise copious passwords. SSO also reduces the likelihood of your user-base exposing your organisation to risk – the proverbial passwords on post-it notes for example.



Three Things to Consider Before Implementing Identity and Access Management

There are many IAM vendors; choosing the best one to fit the needs of your company and your user-base can be daunting. IT Lab can help with this. Bear in mind:

01 Compatibility with your Cloud-based Systems

Not all your cloud-based systems will be the same - their authentication capabilities may differ. Before selecting an IAM solution, check that it's compatible with your key applications. Your vendor's technology must be able to interact with your systems, e.g. by using SAML authentication.

SAML is the standard for exchanging authentication and authorisation data, most commonly between an IAM provider and a cloud service provider. This will help you to decide whether Identity and Access Management is worth the investment.

It's a question of determining what you're going to gain. Having one application that isn't SAML enabled doesn't necessarily mean you shouldn't invest. If the majority are, you'll gain advantages across that set of applications.

02 Ease of Implementation and the Circumstances of your User-base

The less complex, the easier it will be for your business to implement and for your users to consume. Consider the various multi-factor authentication capabilities open to you and how they match the circumstances of your users. For example, if some don't have corporate mobile phones, how will you push out the second factor?

At IT Lab, we find our clients have a common method across their environment because it makes management easier. If necessary, it's possible to mix the authentication methods, e.g. on a device or location basis. This is known as conditional authentication.

03 Do Third Parties Require Access to your Systems?

Perhaps people outside your business require access to your systems. If so, they will require to be issued with Single Sign-on credentials. This can give you greater control over when and what they access. For example, for a set length of time, or to granular information in a subset of your systems.

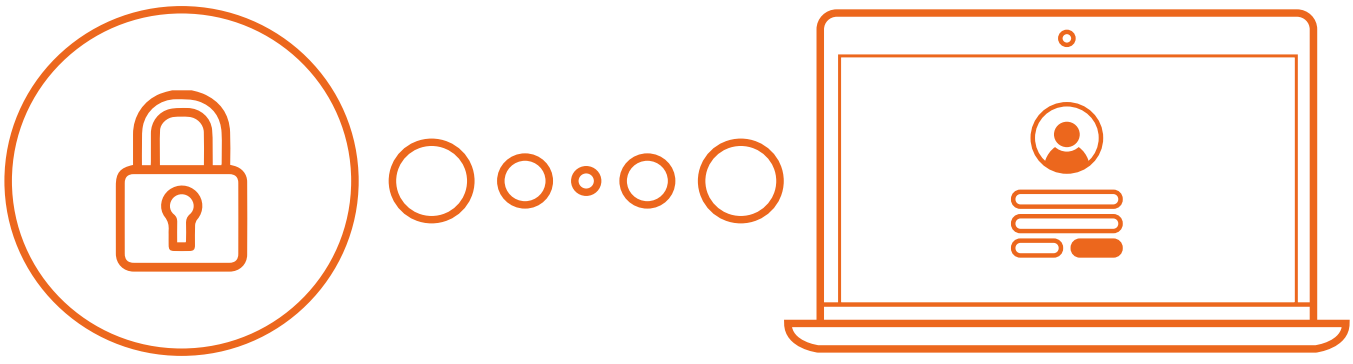
Integrating Identity and Access Management with Wider Security

A combination of external inputs can radically improve your company's security posture and allow you to access high-end expertise which – to deliver in-house - would require significant investment.

Single Sign-on data can be fed into other security monitoring platforms for central management. For example, by a Security Operations Centre (SOC).

By relaying log-in activity to a central control centre, any suspicious or unusual behaviour is detected and reacted to faster than it otherwise would be. Often these key events are overlooked and businesses aren't aware that they have been compromised.

> "From day one, IT Lab demonstrated not only their technical knowledge – which is huge - but their focus on service. Their team took care to understand our challenges before guiding us towards the right solutions. They were frank when explaining the options, and rapidly gained our trust and confidence.
>
> IT Lab are easy to do business with and endlessly supportive.
>
> I highly recommend them to any of my peers in the recruitment space."
>
> **CIO, London based recruitment company**



Security Operations Centre (SOC)

A Security Operations Centre acts as the eyes and ears of your business. It consists of a powerful combination of cybersecurity experts and advanced, multi-layered technologies.

IT Lab's SOC is available at a fraction of the cost, complexity and resource you would need to deliver a comparable model in-house. Our custom-built facility in Manchester includes:

> **Round the clock security monitoring;** watching for attacks and infections.

> In an ocean of threats, our expert **analysis and triaging** ensures attention is focussed when and where it's needed most.

> **Pragmatic, actionable advice** for rapid prevention and / or remediation.

> As appropriate, delivery and/or assistance with the above.

> **Regular updates** and **intelligence sharing**, including direct telephone calls. Options include access to real-time reporting dashboards and mobile alerts.

> **Support with vital compliance**, e.g. GDPR, ISO 27001, Cyber Essentials PLUS etc.

Penetration Testing and Gap Analysis

As well as considering the proactive defence and protection that a Security Operations Centre provides, it's worth exploring the insight that can be gained from assessing your current levels of cybersecurity first. The results of a penetration test or gap analysis often help to support the case for a sustainable, long-term investment in your security.

A penetration test is a point-in-time picture of your defences and security vulnerabilities. You can choose to have any system or element of your infrastructure tested, including:

> Your network

> Web applications – often viewed as the Achilles' heel of cybersecurity

> Your wireless solutions

> Your mobile applications

Penetration testing can be a vital step towards closing the gaps in your IT infrastructure. By conducting a simulated attack, our ethical hackers will identify where your cybersecurity is lacking. Whether it's hardware or software flaws, poor system configuration or even user errors, we can help you stay one step ahead of cybercriminals or malicious insiders.

For a holistic view of how your systems and infrastructure stand-up to real-world threats, a Red Team assessment gives you the most complete picture. In this type of assessment our team of ethical hackers do exactly that, they hack. Our team will replicate the threats specific to the recruitment sector to realistically test your defences.

This first step can also be done through an assessment - or gap analysis - where your IT infrastructure and systems are reviewed to establish if they meet the minimum levels of cyber hygiene every business needs. Recruitment companies often do these things in parallel.

The Psychology of Your User Base

Once you've selected the right method for your technical security controls, it's imperative to get your users on board. Before implementing any modern technology, be aware there's a heartbeat at the other end and never assume your users will automatically comply with your requirements.

There may be a degree of angst as they mistakenly perceive they're being punished, or they may think 'everything's okay, why do I need to change?'

So how do you bring your users with you? It's about education – rather than just telling them what to do, explain your rationale. It's cultural too; anything that improves security should be driven at board level, not solely IT.

Fundamentally, don't impose things. Explain your plans at an early stage.

User Awareness

Despite this fact, the user aspect of security is often overlooked. Cybercriminals exploit this lack of vigilance through social engineering. For example, by persuading employees to divulge their login information or tricking them with a convincing email containing a malicious link. This is known as phishing and can be highly sophisticated.

IT Lab offers interactive online user-awareness courses. To encourage participation, they've been designed to be fun and competitive. We also deliver on-premise workshops for all levels, including your board. The content is compelling and will transform how your users think.

Our training options foster a culture of security by equipping your people with a realistic understanding of the tactics cybercriminals use together with the confidence to deal with them.

About IT Lab

Microsoft Partner
Microsoft
Gold Enterprise Resource Planning
Gold Cloud Productivity
Gold Cloud Platform
Gold Datacenter
Gold Small and Midmarket Cloud Solutions

Microsoft Partner
Microsoft
Gold Collaboration and Content
Silver Messaging
Silver Enterprise Mobility Management

megabuyte TOP 50

QMS ISO 9001 : 2015 REGISTERED

QMS ISO 27001 : 2013 REGISTERED

ITEUROPA 2018 FINALIST

Channel Futures MSP 501 2018 WINNER

Our name means we live and breathe IT. We have teams of experts in every discipline of technology - from IT support to strategy and consultancy - and everything in between. This includes business applications, the cloud and connectivity, and other security solutions and services.

We have eight Microsoft core competencies, placing us in the elite 1% of Microsoft Certified Partners. As you might expect, we hold ISO 9001 and ISO 27001 certifications. We've also achieved a raft of awards and are proud to be among the UK's top three managed service providers.

What does this mean for you and your business? It means that whatever your needs and wherever you are on your journey, we can help. Our ***navigate, integrate, operate*** approach will help your recruitment business make the most of technology and empower your people to be their best.

Would You Like IT Lab's Help to Protect Your Sensitive Recruitment Data?

We hope this brochure has inspired you to explore the potential of the many transformative technologies and services available today.

To connect with Michael Bateman and his team, you're welcome to contact us today.

Call: 0333 241 7689

Email: hello@itlab.com

Visit us at www.itlab.com

London
40 Bernard Street
Bloomsbury
London
WC1N 1LE

Manchester
Lowry Mill
Lees St
Swinton
Manchester
M27 6DB

www.itlab.com