iGOV survey

Access Management: Improving Security Across the Public Sector

SURVEY REPORT 2019

Survey Partners

HelloID
Cloud. Identity. Access.

TABLE OF CONTENTS

INTRODUCTION

The challenge to keep our most sensitive information gets more complex as technology advances. The amount of sensitive data we collect, increasingly sophisticated cyberattacks and the risk of human error all play their part, and organisations must be able to manage these threats. And to do this, the ability to effectively and securely identify users and manage access to systems is critical.

According to the National Cyber Security Centre (NCSC) in their guidance on identity and access management; "It is important that companies appropriately identify anyone who could have access to your systems at the first point of contact, establishing their true identity and a method of future authentication." [1]

Yet this process isn't always straightforward. As organisations look to embrace more flexible working arrangements, including working from home and Bring Your Own Device (BYOD) schemes, organisations should think about using diverse types of authentication, such as biometrics, multi-factor authentication and at its very basic level, passwords.

NCSC say, "When designing an authentication approach, it is important to consider both the physical environment which the user will perform their authentication from, and the trustworthiness of the devices they will use to perform that authentication." [2]

Yet its not just data and employees that organisations need to contend with. In late 2017, Gartner's Planning Guide for Identity and Access Management noted that "the shifting users, applications and management to the cloud, and the acceleration of IT innovation, has forever altered the IAM landscape. Technical professionals must focus on IAM initiatives that deliver rapid time to value but avoid 'technical debt'."

1. National Cyber Security Centre, a part of GCHQ, Introduction to identity and access management, 23 Jan 2018, https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management
2. National Cyber Security Centre, a part of GCHQ, Introduction to identity and access management, 23 Jan 2018, https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

As the public sector strives to keep up with developments in technology, people management and data regulations, iGov Survey teamed up with IAM experts, HelloID, to examine the role of identity and access management in security strategies across the sector.

In particular, our study explores:

- the areas currently thought to be having the biggest impact on security strategies;
- the biggest concerns surrounding identity and access management; and
- what organisations believe will present their biggest opportunities in the year ahead.

ABOUT HelloID

HelloID is a wholly owned subsidiary of Tools4ever BV, a privately held Dutch company and one of the largest vendors in Identity Governance & Administration with more than 5 million managed user accounts.

Since 1999 the company has developed and delivered several software solutions and consultancy services such as User Provisioning, Downstream Provisioning, Workflow Management, Self-Service and Access Governance (RBAC). In the area of Password Management, Single Sign-On and Self-Service Password Reset have proved highly successful.

The company's Identity Governance & Administration (IGA) solutions are installed in both corporate and public sector organisations, ranging in size from 300 to over 200,000 user accounts.

Providing secure access to an organisation's data is a multi-faceted and ever-changing process – one that the company fully understands. Identity Governance & Administration (IGA) is a complex process, but we can streamline it. Complete IGA solution can be delivered in weeks rather than months.

With a simple, direct approach, our professional services teams can enable organisations to become more efficient and secure using any combination of the suite of applications.

HelloID
Cloud. Identity. Access.

For nearly 20 years, the company has been dedicated to developing and delivering these highly standardised IGA solutions that are as easy to implement as they are to manage. The company is focused on quickly providing greater efficiency and improved security at a competitive price point that delivers outstanding value at a low cost of ownership and outstanding ROI.

SURVEY METHODOLOGIES AND RESPONDENTS' PROFILE

This survey was conducted by iGov Survey in partnership with HelloID. The project ran from Friday 14 December 2018 to Wednesday 30 January 2019.

Survey respondents represented a broad cross-section of roles across the public sector. This included: Architect, Board Secretary, Business Development, Clinical, Commissioning, Computer Security, Corporate Services, Customer Services, Digital, Engineer, Facilities & Estates, Finance Management, General Manager, Human Resources, Information, Information Governance, IT Management, IT Technical Lead, Library, Operations, Partnerships, Programme Management, Project, Scientific, Senior Manager, Service Delivery, Strategy, Technical Services, and Transformation/Change Management.

75 individuals took part in our survey, representing 72 unique organisations across the public sector. There was no inducement to take part in the survey, and HelloID was not introduced as the survey partner.

The results displayed throughout this report are based on those who fully completed the questionnaire and are displayed as a percentage of this group, unless explicitly stated otherwise.

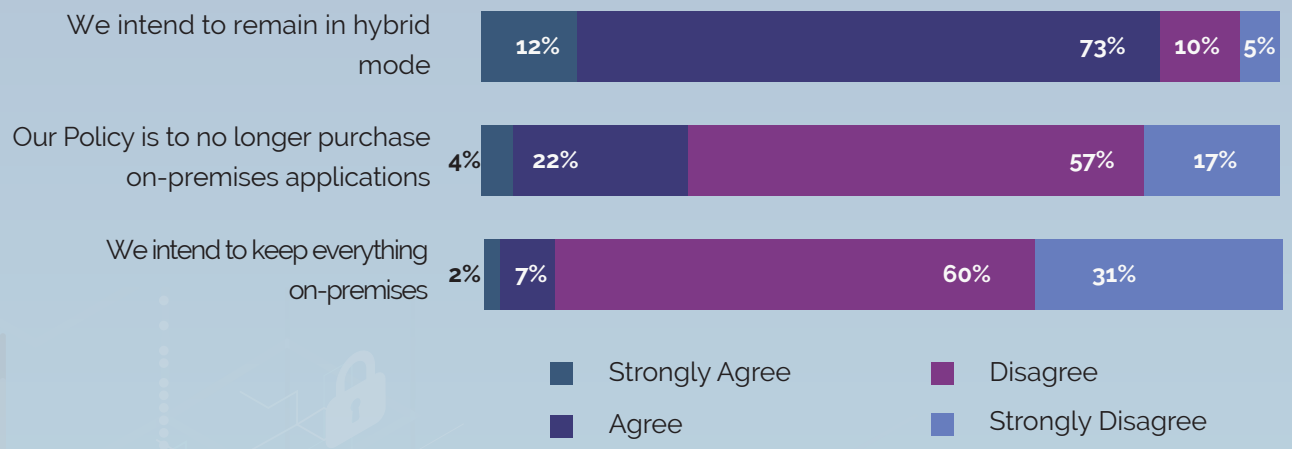
KEY FINDINGS

1 While there is still a heavy reliance on on-premise solutions, there is growing adoption of Cloud.

Most participants (73%) report that their organisation intends to remain in 'hybrid mode', using a mixture of traditional and cloud-based infrastructure and solutions. This is further supported by more than half (57%) who disagreed with the statement; 'our policy is to no longer purchase on-premise applications'. Yet 90% also disagreed with the notion of maintaining everything on premise, suggesting that many are opting for a 'half-way' compromise

Figure 1:

Thinking about IT and data security, to what extent do you agree with the following statements?



A quarter of participants don't know or are unsure of whether they have a formal strategy for the adoption of cloud technologies (32%).

However, more reassuring is the fact that 68% of participants are aware that the organisation they work for has a cloud adoption strategy.

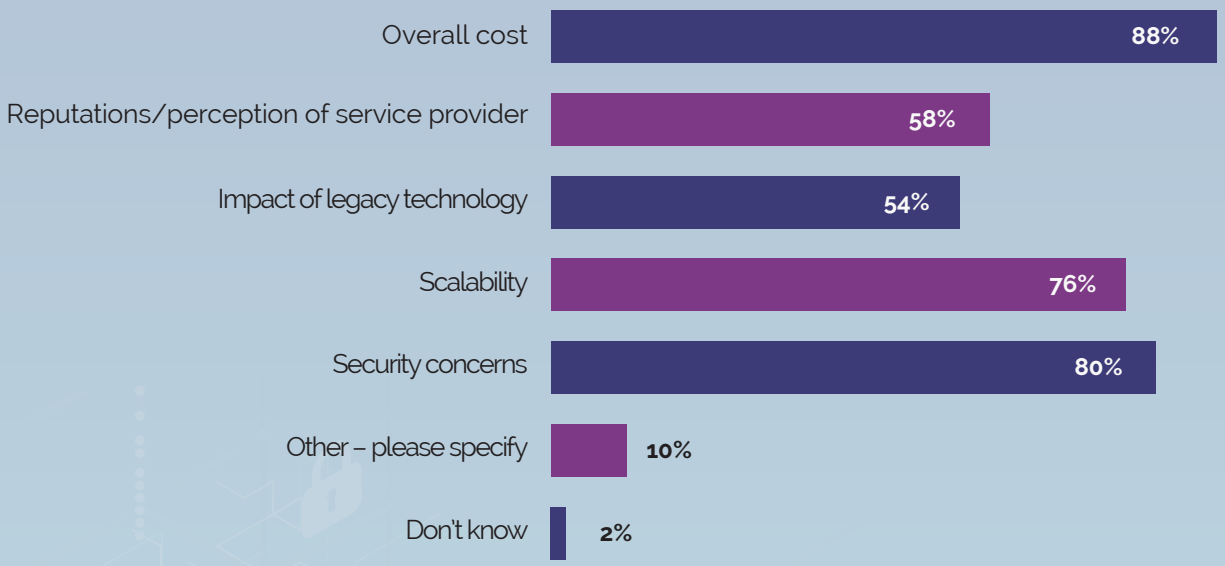
Figure 2:

Does your organisation have a strategy of the adoption of Cloud technologies?

The biggest considerations for these strategies are overall costs (88%), and security (80%), which comes as no surprise, as historically this is a nagging point for cloud. Yet as technology advances, security is now fast becoming a selling point for cloud, which can simultaneously be significantly cheaper and more secure.

Figure 3:

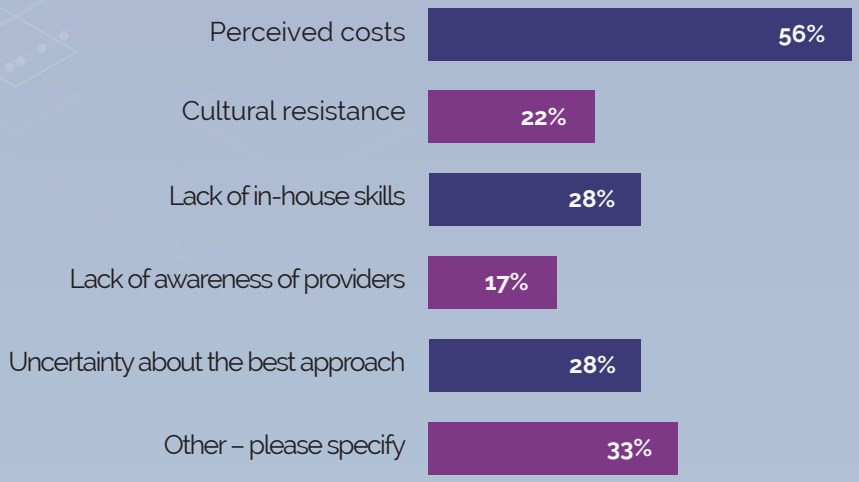
Which of the following areas are considered as a part of this strategy?



Uncertainty about the best approach is also seen as a significant barrier to the adoption of cloud, with just over a quarter stating this issue (28%) alongside a lack of in-house skills to adopt. These, perhaps predictably, follow perceived costs (56%) as main concerns across the sector.

Figure 4:

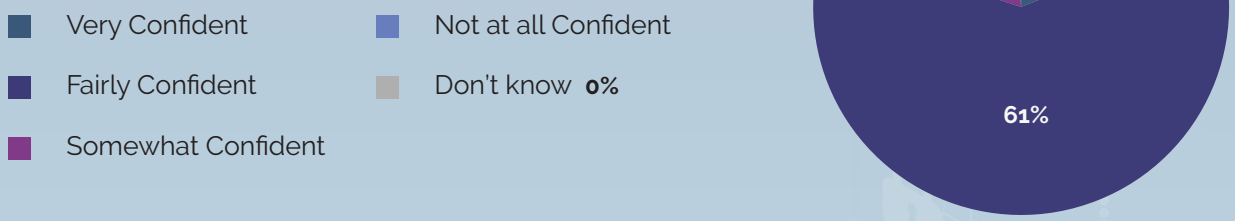
What are the main barriers to the adoption of cloud technology in your organisation?

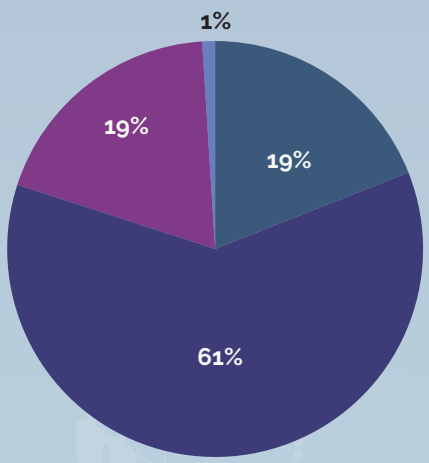


2 **Less than a fifth of those who took part in the survey (19%) are very confident in their organisations ability to secure their systems and data effectively.**

Figure 5:

How confident are you that your organisation is able to secure your systems and data effectively?

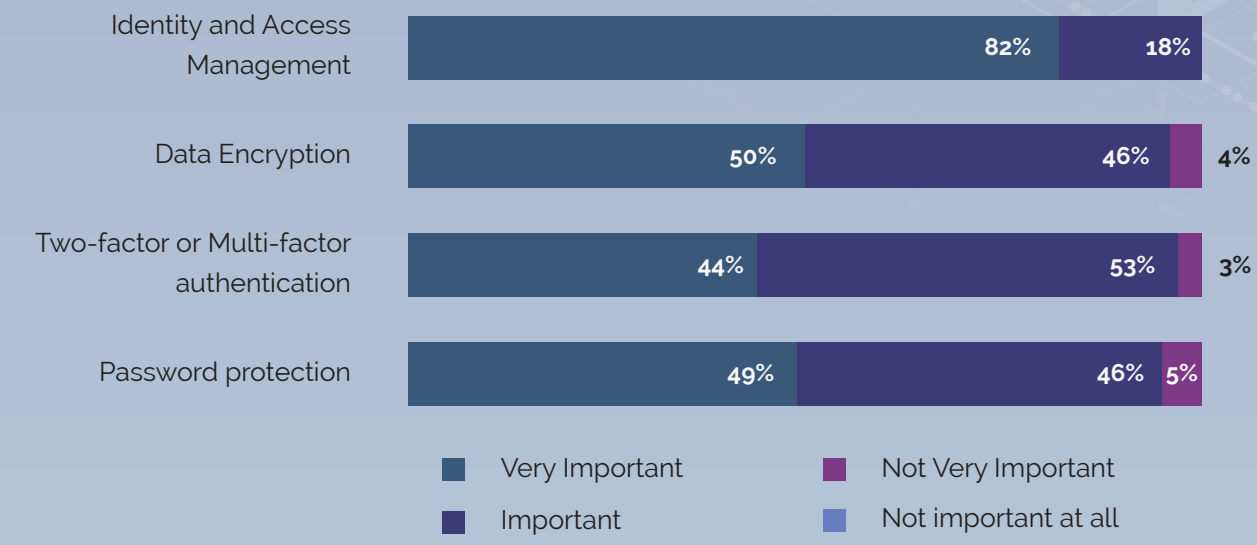




More than three-quarters of participants said that Identity and Access Management is the most important access for security (82%), with its closest competitor being data encryption at 50%. Just less than half believe that password policies are very important (49%), with the same being said for two-factor or multi-factor authentication (45%).

Figure 6:

How important do you believe the following security aspects are with regard to protecting networks and data?



Looking at the areas which have the biggest impact on their organisation's security strategies, increasingly sophisticated cyber-attacks are a concern (74%). Almost three-quarters (73%) are also concerned about the need to enable employees to work remotely and flexibly across their organisation.

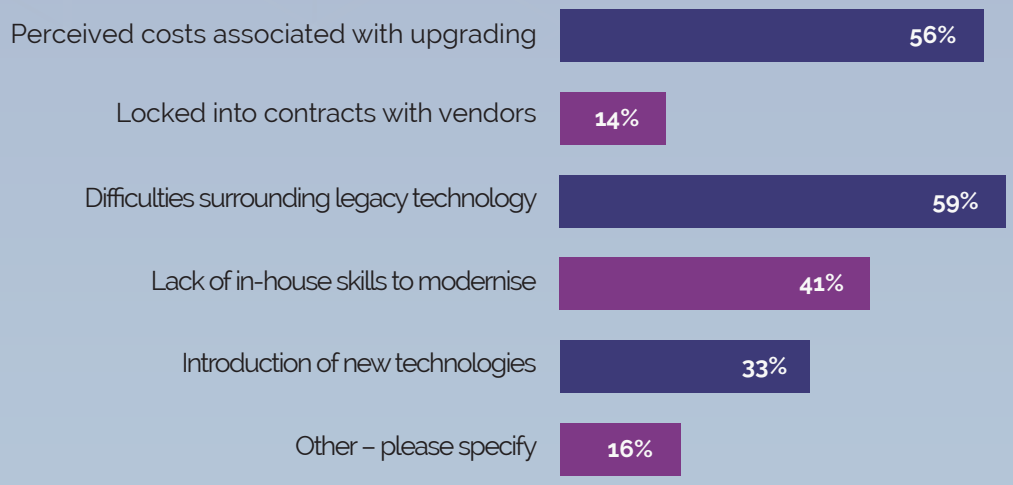
Figure 7:

As public-sector organisations look to modernise and meet the demands of digitally engaged staff and citizens, which of the following areas do you believe are having the biggest impact on your organisations security strategies?

More than half of participants said difficulties surrounding legacy technology (59%) is one of the biggest challenges organisations face. It also comes as no surprise that 56% of participants said that the perceived costs associated with upgrading is a challenge, with 49% saying that a lack of in-house skills is a challenge they face.

Figure 8:

In your opinion, which of the following areas present the biggest challenges to your organisation when it comes to IT and data security?



3 Nearly two-thirds don't have or are not aware of the capability within their organisation to access a single overview of access permissions per user (65%).

Figure 9:

Does your organisation have a single overview of access permissions per user?

Looking at requirements for organisations' helpdesks, password resets are the most common (57%), closely followed by application access (50%), suggesting that many IT helpdesks across the sector could be losing valuable time on areas that could be easily automated. Interestingly, a quarter of participants have between 6 and 20 username and password combinations to remember, with 65% stating they have just 1 to 5 combinations to remember.

Figure 10:

Of the following list, what are the most common requirements and requests to be made to your organisations help desk?

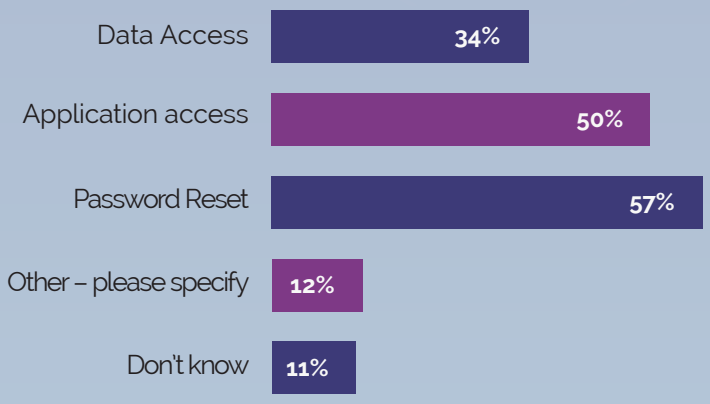
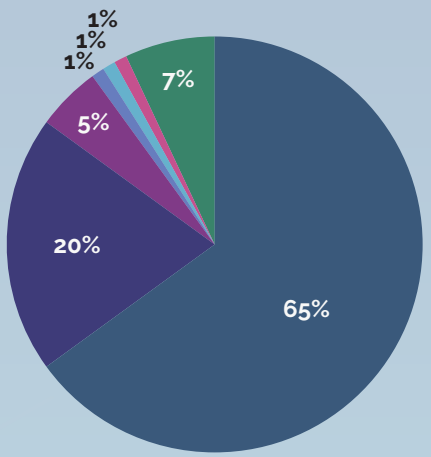


Figure 11:

Approximately, how many username and password combinations does your average user have to remember?



4 When it comes to having a formal strategy for identity and access management, less than half of participants (49%) said they have a formal strategy concerning this.

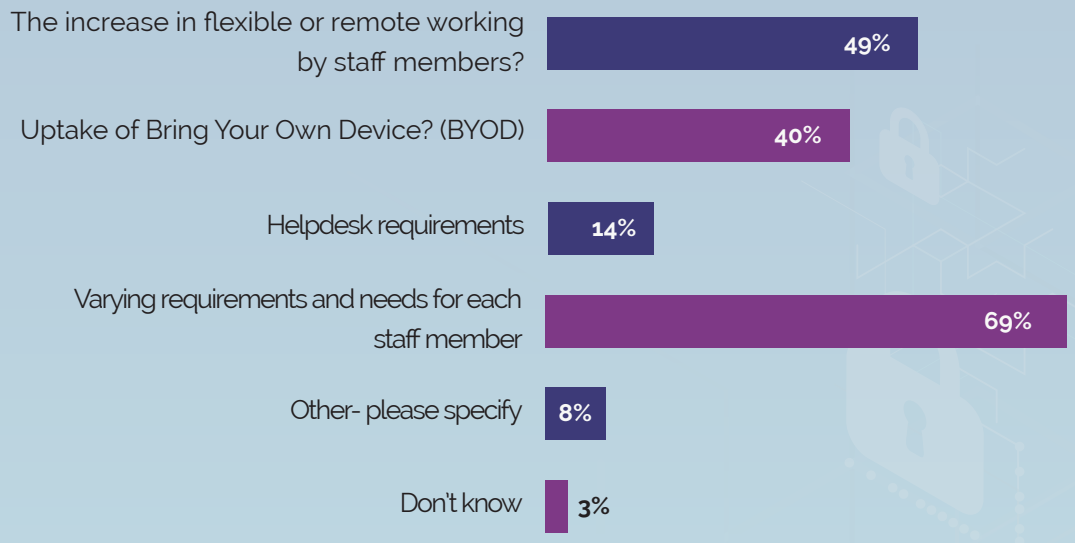
However, over two-thirds (69%) believe that the varying requirements and needs of each staff member poses a significant challenge for their strategy, as well as the uptake on BYOD schemes (40%) and the increase for flexible or remote working by staff members (49%). When it comes to those who have a strategy, over three quarters, 72%, are reviewing and renewing this in the next year, and when it comes to those with no strategy, half of participants intend to implement one in the coming year.

Figure 12:

Does your organisation have a formal strategy concerning identity and access management (IAM)?

Figure 13:

Which of the following areas do you believe pose a significant challenge for your IAM strategy

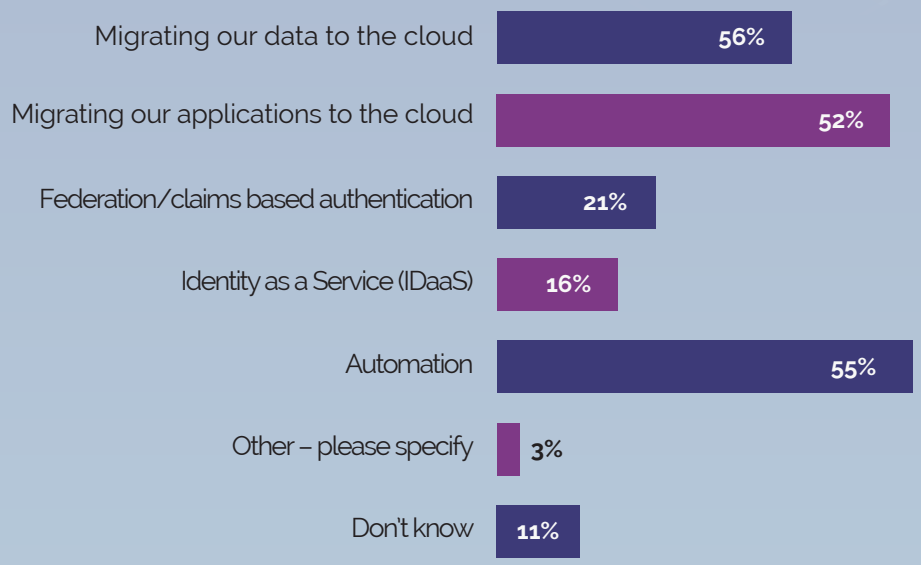


5 Looking forward, 55% of participants believe that automation presents a significant opportunity for their organisation

This is closely followed by half who say migrating their applications to the cloud presents a significant opportunity. Migrating data to the cloud is also a significant opportunity for organisations, according to 39% of our participants.

Figure 14:

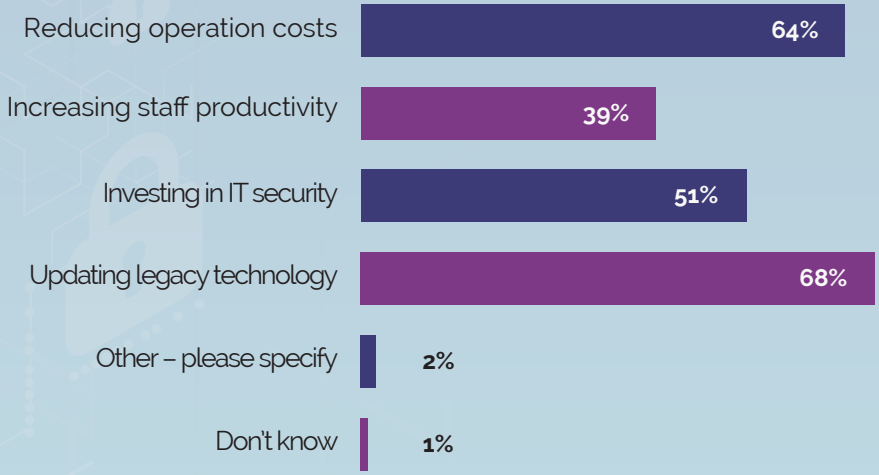
Looking ahead, which if the following areas do you believe present the biggest opportunities for your organisation?



Updating legacy technology is the biggest challenge going forward (68%), this is closely followed by 64% who state reducing operation costs is a challenge, and it is also good to see that half of participants, 51%, are also investing in IT security.

Figure 15:

Conversely, what do you believe will be your organisation's biggest challenges?



CONCLUSION

By HelloID

According to statistics published by EuroSat in 2018, British enterprises boast a relatively high rate of cloud adoption, with 41.9% of organisations adopting some form of cloud service, against an EU average of 26.2%. However, according to the report, the cloud has been adopted mostly for Email hosting and file storage. Interestingly, only 55% of those who have already adopted the cloud are hosting advanced cloud services such as accounting software or CRM applications.

So what will 2019 bring us?

We wanted to conduct this survey so see if attitudes to the cloud are changing for 2019. With 73% of respondents intending to stay in Hybrid Mode, it's clear that cloud computing is yet to peak in the UK. This is re-enforced by 74% of you still happy to purchase new applications to run in house. With 58% of organisations not knowing "who has access to what" it's not surprising that more data has not been moved to the cloud.

Yet despite the clear winner for Hybrid Networks, IdM, 2FA and Password Policies are still of huge importance to security. Rather than their focus being on securing true cloud services, 73% of you are also concerned about the need to enable employees to work remotely and flexibly, without compromising security.

56% perceive the cost of cloud computing being a big barrier, yet 52% still believe that migrating applications to the cloud will bring the biggest opportunities for the organisation.
As an Identity and Access Management company, one statistic that did jump out to us was that 69% of you believe that the "Varying requirements and needs for each staff member" poses a significant challenge to your IAM Strategy.

For an enterprise IAM solution to address these issues, it requires a number of characteristics:

Enhanced Authentication – Typical authentication requires only a user name and password, sometimes supported by two factor authentication. To improve security authentication should be context aware, controlling access to applications and data by origin, place, time and device

Single Sign-On – Users accessing multiple applications with differing password complexity rules will often resort to insecure ways record them. Single sign-on allows users access to their application landscape

User Provisioning – Automating the creation, amending and disabling/deleting of network accounts ensures accounts are created correctly and that only necessary access is granted (known in the industry as RBAC). Leavers' accounts are guaranteed to be disable/deleted to meet auditing and compliance requirements

Data Management – Internal knowledge of who has access to what is a grey area. Data management allows the natural owners of data and applications to be identified and control/amend/deny access

Service Automation – Users need to be able to request access to network resources and be guaranteed correct assignment via product owner authorisation

HelloID is a Microsoft hosted Service Portal that supports all of the identified requirements of an IAM installation. It complies with the hybrid cloud model currently in favour and is competitive in comparison to traditional on-premise installations.

Our platform is one of the first in its kind to deliver an identity ecosystem; Access Control, SSO, Self Service, Data Management, Delegation & User Life Cycle Management.

If you would like us to advise you on how we can streamline your processes, please contact us at **www.HelloID.co.uk**

HelloID
Cloud. Identity. Access.

APPENDIX 1: SURVEY QUESTIONS

Grid
Thinking about IT and data security, to what extent do you agree with the following statements?

Question
Our policy is to no longer purchase on-premises applications

Answer	Percent
Strongly agree	4%
Agree	22%
Disagree	57%
Strongly disagree	17%

Question
We intend to remain in hybrid mode

Answer	Percent
Strongly agree	12%
Agree	73%
Disagree	10%
Strongly disagree	5%

Question
We intend to keep everything on-premises

Answer	Percent
Strongly agree	2%
Agree	7%
Disagree	60%
Strongly disagree	31%

Question
We are moving all infrastructure and services to the cloud

Answer	Percent
Strongly agree	3%
Agree	15%
Disagree	63%
Strongly disagree	19%

Question
As public sect ororganisations look to modernise and meet the demands of digitally engaged staff and citizens, which of the following areas do you believe are having the biggest impact on your organisat ion's security strategies?

Answer	Percent
The need to enable employees to work remotely and flexibly	73%
Increasingly sophisticated cyber-attacks	74%
The introduction of modern technologies, such as Cloud	53%
Other - please specify	15%
Don't know	0%

Question
In your opinion, which of the following areas present the biggest challenges to your organisation when it comes to IT and data security? Please tick all that apply.

Answer	Percent
Perceived costs associated with upgrading	56%
Locked into contracts with vendors	14%
Difficulties surrounding legacy technology	59%
Lack of in-house skills to modernise	41%
Introduction of new technologies	33%
Other - please specify	16%
Don't know	0%

Grid
How import ant do you believe the following security aspects are with regard to protecting your networks and data?

Question
Identity and access management

Answer	Percent
Very important	82%
Important	18%
Not very important	0%
Not at all important	0%

Question
Data encryption

Answer	Percent
Very important	50%
Important	46%
Not very important	4%
Not at all important	0%

Question
Remote wipe

Answer	Percent
Very important	19%
Important	66%
Not very important	15%
Not at all important	0%

Question
Two-fact or or multi-factor authentication

Answer	Percent
Very important	45%
Important	53%
Not very important	3%
Not at all important	0%

Question
Password policies

Answer	Percent
Very important	49%
Important	46%
Not very important	5%
Not at all important	0%

Question
How confident are you that your organisation is able to secure your systems and data effectively?

Answer	Percent
Very confident	19%
Fairly confident	61%
Somewhat confident	19%
Not at all confident	1%
Don't know	0%

Question
Approximately, how many username and password combinations does your average user have to remember?

Answer	Percent
1 to 5	65%
6 to 10	20%
11 to 20	5%
21 to 30	1%
More than 30	1%
Don't know	7%

Question
Of the following list, what are the most common requirements and requests to be made to your organisation's IT helpdesk? Please tick all that apply.

Answer	Percent
Data access	34%
Application access	50%
Password reset	57%
Other - please specify	12%
Don't know	11%

Question
Currently, is your organisation able to manage access to systems and sensitive data through the following criteria? Please tick all that apply

Answer	Percent
Location	54%
Device	61%
IP address	64%
Date/Time	32%
We are not currently able to do this	12%
Other - please specify	8%
Don't know	5%

Question
Does your organisation have a single overview of access permissions per user?

Answer	Percent
Yes	35%
No	58%
Don't Know	7%

Question
Does your organisation have a formal strategy concerning identity and access management (IAM)?

Answer	Percent
Yes	49%
No	40%
Don't Know	11%

Question
Which of the following areas do you believe pose a significant challenge for your IAM strategy? Please tick all that apply.

Answer	Percent
The increase in flexible or remote working by staff members	49%
Uptake of Bring Your Own Device (BYOD)	40%
Helpdesk requirements	14%
Varying requirements and needs for each staff member	69%
Other - please specify	8%
Don't know	3%

Question
Is your organisation planning to review its strategy in the coming:

Answer	Percent
Three months	5%
Six months	14%
Twelve months	53%
Post twelve months	17%
Other - please specify	3%
Don't know	8%

Question
Is this something your organisation is considering implemenying in the coming 12 months?

Answer	Percent
Yes	50%
No	27%
Don't Know	23%

Question
Looking ahead, which of the following areas do you believe present the biggest opportunities for your organisation? Please tick all that apply.

Answer	Percent
Migrating our data to the cloud	39%
Migrating our applications to the cloud	52%
Federation/claims based authentication	21%
Identity as a Service (IDaaS)	16%
Automation	55%
Other - please specify	3%
Don't know	11%

Question
Conversely, what do you believe will be your organisation's biggest challenges? Please tick all that apply.

Answer	Percent
Reducing operation costs	64%
Increasing staff productivity	39%
Investing in IT security	51%
Updating legacy technology	68%
Other - please specify	2%
Don't know	1%

Question
Does your organisation have a strategy for the adoption of Cloud technologies?

Answer	Percent
Yes	68%
No	24%
Don't Know	8%

Question
Which of the following areas are considered as part of this strategy? Please tick all that apply.

Answer	Percent
Overall cost	88%
Reputation/perception of service provider	58%
Impact of legacy technology	54%
Scalability	76%
Security concerns	80%
Other - please specify	10%
Don't know	2%

Question
What are the main barriers to the adoption of Cloud technology in your organisation? Please tick all that apply.

Answer	Percent
Perceived costs	56%
Cultural resistance	22%
Lack of in-house skills	28%
Lack of awareness of providers	17%
Uncertainty about the best approach	28%
Other - please specify	33%
Don't know	0%

Question
Do you currently conduct regular security audits across your organisation and, if so, how often do you complete these?

Answer	Percent
Monthly	16%
Every other month	5%
Every six months	19%
Annually	22%
Ad hoc, as and when needed	20%
Other - please specify	7%
Don't know	11%

Question
Thinking about identity and access management , which of the following products do you see as the market leader? Please tick all that apply.

Answer	Percent
HelloID	1%
Microsoft Azure	53%
Okta Identity Cloud	5%
IBM Security Identity and Access Assurance	0%
Oracle Identity Cloud Service	5%
Other - please specify	5%
Don't know	41%

APPENDIX 2: PARTICIPATING ORGANISATIONS

Central Government
Home Office
Met Office
Office for National Statistics
Parliamentary Digital Service

Charity
Cardinal Hume Centre
Chartered Institute of Environmental Health
Cripplegate Foundation
Derbyshire Wildlife Trust
Rothamsted Research Limited
Sheffield City Trust
St Basils
The Fremantle Trust
Together Trust
United Response

Clinical Commissioning Groups
NHS Dorset CCG

Colleges of FE
Birmingham Metropolitan College
Blackpool and the Fylde College
Bolton Sixth Form College
Brockenhurst College
Eastleigh College
Edinburgh College
Fashion Retail Academy
Havering Sixth Form College
Herefordshire and Ludlow College
Myerscough College
North East Scotland College
NPTC Group
Shrewsbury College
South Lanarkshire College
Union Theological College
University of the Highlands and Islands
Weston College

Housing Associations
Bield Housing Association
Coastal Housing Group
Guinness Partnership
Lewisham Homes
Milnbank Housing Association
Optivo
Osprey Housing Moray
Phoenix Community Housing
Soha Housing
Vale of Aylesbury Housing Trust

Local Government
Allerdale Borough Council
Birmingham City Council
Brentwood Borough Council
Chelmsford City Council
Cumbria County Council
Epping Forest District Council
Epsom and Ewell Borough Council
Hartlepool Borough Council
Islington Council
Oxfordshire County Council
Preston City Council
Sheffield City Council
Shropshire Council
South Somerset District Council

NHS
Abertawe Bro Morgannwg University Health Board
Ashford and St Peter's Hospitals NHS Foundation Trust
Belfast Health and Social Care Trust
Gloucestershire Hospitals NHS Foundation Trust
Lancashire Care NHS Foundation Trust
NHS England
Northampton General Hospital NHS Trust
Oxford University Hospitals NHS Foundation Trust
The Health Informatics Service NHS
The Royal Liverpool and Broadgreen University Hospitals NHS Trust
The Royal Orthopaedic Hospital NHS Foundation Trust
Wirral University Teaching Hospital NHS Foundation Trust
Worcestershire Acute Hospitals NHS Trust

Non Departmental Public Bodies
Natural History Museum
The Pensions Regulator

University
City, University of London
De Montfort University
Northumbria University
University of Aberdeen
University of Brighton
University of Derby
University of Exeter
University of Glasgow
University Of Huddersfield
University of Reading
University of St Andrews
University of the West of Scotlandr

ACKNOWLEDGEMENTS

The survey team at iGov Survey would like to take this opportunity to thank all of those who were able to take part in our research, particularly those who found the time to offer additional insights through additional comments. We would also like to thank our survey partner, HelloID, for their assistance in compiling the questions, scrutinising the responses and analysing the results.

To contact the iGov Survey team:
Email: sandra.peet@bipsolutions.com
Tel: 0845 094 8567
Address: FAO Sandra Peet, Pacific House, Pacific Way, Digital Park, Salford Quays, M50 1DR

iGOV survey

iGOV survey

web: www.igovsurvey.com email: enquiries@igovsurvey.com tel: 0845 094 9567