

Record attendance of Chilean executives at ninth Chile Day in London

The strong relationship between the UK and Chile was once again stressed by the presence of over 500 investors and business persons, as well as officials from the Chilean government, at Chile Day 2019 held in London on 10 and 11 September.

Chile Day aims to strengthen ties between the representatives of Chilean capital markets and the City of London. It presents Chile as an investment destination and platform for funds across Latin America. For the UK, Chile Day is an opportunity to show the benefits of investing in one of the most important financial cities of the world.

For 9 years in a row, Chile Day was held in London, in partnership with:

- the Chilean Ministry of Finance
- the British Embassy in Santiago
- the Embassy of Chile in London
- InBest Chile (main organiser)
- Pro Chile (the export promotion bureau of Chile)

There were also side events held at the Bank of England, the London Stock Exchange and the Foreign and Commonwealth Office (FCO).

The focal points of this year's Chile Day were:

- cyber security
- green finance
- fintech
- venture capital

Signature of memorandum of understanding

The highlight of Chile Day 2019 was the signature of a memorandum of understanding between the UK and Chile at the Foreign and Commonwealth Office. The instrument, signed by FCO Minister of State Andrew Stephenson MP and Chilean Minister for Finance Felipe Larraín, will allow the 2 countries to further collaborate in this sector, especially in the fields of data protection and hacking prevention.

At the event was also present Chile's Presidential Adviser for Cyber security, Mario Farren, who also held meetings with officials from the National Cyber Security Centre, the FCO, the Home Office, Cabinet Office and Department for Business, Energy and Industrial Strategy (BEIS).

Further information

If you want to know more about Chile Day, contact [Gabriel Henriquez](#), Trade and Economics Policy Officer, British Embassy, Santiago.

For more information about the events and activities of the British Embassy in Santiago, follow us on:

[UK statement on safety of journalists of the media at HDIM 2019](#)

Madam Moderator, Ladies and Gentlemen,

The United Kingdom fully aligns ourselves with the statement given by Sweden on behalf of the EU and would like to add some comments in our national capacity.

I outlined yesterday how the Global Campaign for Media Freedom has two objectives: to mobilise a global spotlight on media freedom and to increase the costs to those abusing it.

We are now working actively to deliver on the initiatives launched at the conference. We would welcome your participation and ideas on these five areas:

First, we are encouraging more countries to sign the campaign Global Pledge, developed jointly with Canada. By doing so, Governments are committing to safeguard media freedoms and to protect journalists, and to hold themselves to the highest standards. Across the OSCE region, we already have 14 countries signed up. We are encouraging others to do so.

Second, we will be launching the new Media Freedom Coalition next week at a Ministerial event at the UN General Assembly in New York on 25 September. Members of the Coalition – those governments who have signed the Pledge – will speak out and lobby on specific cases, make collective statements in international fora and provide peer review to encourage progress on media freedom. If your government is interested in joining the Coalition, please contact the UK Delegation.

Third, we encourage your support in providing financial contributions to the Global Media Defence Fund, administered by UNESCO, which will train, support and provide legal assistance to journalists. With thanks to Slovenia and Lithuania for their commitments already to join the UK and Canada on this important initiative.

Fourth, we are responding to the appeal by the UN Secretary-General, OSCE

Representative and other organisations to take preventative action at the national level by encouraging all countries to develop National Action Plans on the safety of journalists. We now have an international taskforce, led by UNESCO together with the OSCE, to support countries with best practice. Please do approach those organisations and the UK if your country might wish to develop such a plan.

In the UK, we have just started work on our own national committee and action plan which will examine current protections offered to journalists in the UK, and consider how to work together to reinforce them. The Committee will champion journalists' ability safely to carry out their important roles in society and to continue to hold the powerful to account. This is part of our broader commitment to ensuring the future sustainability of high-quality, public interest news. We are happy to share our experience and arrange exchange visits between media professionals and the bodies that oversee the media.

Fifth, the Foreign Secretary's Special Envoy Amal Clooney has convened an independent panel of prominent legal experts to help countries strengthen their legal protections to enable the functioning of a free media and prevent and reverse abuses and violations of media freedom. We encourage your governments to draw on support from the Legal Panel.

Madam Moderator,

We are grateful to the OSCE Representative for the Freedom of the Media and to civil society, journalists and media actors for their work to promote and protect media freedom. We invite you to discuss these issues further at the side event being held by the UK and Canada on legal safety of journalists at 1815 in room 1 immediately following the afternoon plenary session.

Thank you.

Hackney Council's approach to moving to a cloud-first model from the PSN

This case study is part of guidance on [moving to modern network solutions and away from legacy networks](#).

Objective

The London Borough of Hackney wanted to migrate as many of its services as possible from the Public Services Network (PSN) to the internet. Hackney wanted to use the internet to provide:

- an easier and a more convenient user experience
- a more secure and cost effective way of sharing data with other organisations
- its IT team with a way to constantly monitor compliance and network security to manage issues instead of waiting for scheduled checks like penetration tests

The migration included moving email to Google's G Suite.

Background

Hackney used the PSN to:

- let staff connect to the Joint Asset Recovery Database (JARD) – a national database used by financial investigators, prosecutors and enforcement staff
- let staff send email using gsi.gov.uk addresses
- run the Domain Name System (DNS) to support JARD and email
- access Department of Work and Pensions (DWP) services
- provide onward connectivity to the NHS Health and Social Care Network (HSCN)

Hackney still uses the PSN to access JARD and services like Blue Badge.

How Hackney moved to the internet

The council moved away from government .gsi email domains and implemented Transport Layer Security (TLS) in response to the [securing government email guidance](#) and upcoming decommission of the GCSx email service.

Hackney's IT department has around 100 staff, supporting 3,500 users across the council, and occasionally uses third-party suppliers. The team had lots of experience so all migration activity was carried out in-house.

Hackney now forces a TLS connection to all the main public sector domains (gov.uk, police.uk, nhs.net, mod.uk, cjsm.net). If an email fails to deliver, the sender would get a non-delivery report, but the IT team has not seen this happen. Hackney staff know they should contact their internal service desk if this happens so they can get help to try again or use a different route.

The IT team is now working to further enhance their security practices through introducing a 'red team' approach. The team will proactively scan the external interfaces of services and imitate the steps a hacker might take to gain access to identify risks so that mitigating actions can be taken swiftly.

Hackney also uses the National Cyber Security Centre's (NCSC's) [Mail Check](#) and [Web Check](#) tools, which help increase security across government by providing additional assurance against services that Hackney presents externally.

Hackney is also working to provide access to on-premise services, such as their intranet, service desk portal, and finance system, using the internet, via any standard browser. This will allow users who authenticate themselves successfully to access services from anywhere. If a corporate service presented over the internet allows offline access, then users will require a trusted device.

Challenges of migrating to the internet

One of the biggest challenges of migrating to the internet is managing a centralised identity and authentication approach. Hackney would like to encourage interoperability. However, this is only possible with systems that are designed to work with [open standards](#).

For example, Hackney would like to help staff access legacy applications from anywhere with a single sign-on with [Microsoft Internet Information Services](#) (IIS) over the web.

Hackney introduced a [reverse proxy](#) to:

Before plugging any service into its Security Assertion Markup Language (SAML) authentication solution, the team first have to add the service to their identity provider to authenticate users. In some cases, this procedure will only work if no other backend requests are made through the service using old authentication types. If the service uses old authentication types like [NTLMv2](#), it's possible to end up with a situation where users can successfully authenticate to what is now a broken service.

The IT team will now require all future services to support the SAML protocol or Open Authorisation (OAuth) for end user authentication and access control. However, many of Hackney's legacy services do not support these. The council took a couple of approaches to protecting these services while still providing them to the internet by using:

- multi-factor authentication for all internet facing services storing [OFFICIAL information](#)
- a cloud identity service to simplify the end user experience

Hackney tried to use a native web application to present legacy applications. If that is not possible they use VMware to present a Windows application, or virtual desktop infrastructure if the application still needs to integrate with other Windows services.

In all cases, the team still present everything through HTML5 so it feels more like a web service to end users.

Benefits of the migration

Since migrating away from the PSN to the cloud, Hackney Council has:

- improved reliability and provided more flexible services for end users
- started to remove PSN-related infrastructure, which is helping to reduce data centre costs and IT administration effort
- improved security through mandating industry standard security controls and NCSC guidance

Lessons learned from the migration

Hackney found it valuable to run planning workshops to help:

- agree key principles
- talk about proposed solutions
- avoid forcing preconceived ideas and plans onto teams
- highlight the benefits of the migration to the cloud
- get buy-in from across the organisation

The team found that getting backing from an impartial source like a Chief Technology Officer or a senior architecture colleague was important. This made sure the project was supported effectively and was not seen as just a security-led activity.

During the migration, Hackney found some suppliers had not yet caught up with the way government now approaches [technology and security](#). The council had to push some vendors to use open standards and provide cloud-based solutions. For example, Hackney wanted cloud-connected printers but found this difficult to explain to some suppliers and is still in the middle of procuring these.

Outcomes of the migration

Hackney switched to a cloud-based email service by following the [GOV.UK secure email guidance](#). This process took about 4 months after the business case and budget was approved. Most of the migration complexity centred on deciding if archive mailboxes and distribution lists were still needed.

Hackney holds a current PSN compliance certificate and will continue to use the PSN for services such as Blue Badge and connecting to DWP for policy updates and queries on revenues and benefits.

The council will continue to migrate to web and mobile technologies as part of its adoption of a [zero trust architecture](#).

For more information on how to migrate to modern networks you can email psnservicedesk@digital.cabinet-office.gov.uk.

Statistical data set: Tuberculosis (TB) in cattle in Great Britain

Detailed statistics on Tuberculosis (TB) in cattle in Great Britain with regional breakdowns.

National Statistics: Latest national statistics on tuberculosis (TB) in cattle in Great Britain – quarterly

Quarterly statistics on tuberculosis (TB) in cattle in Great Britain.