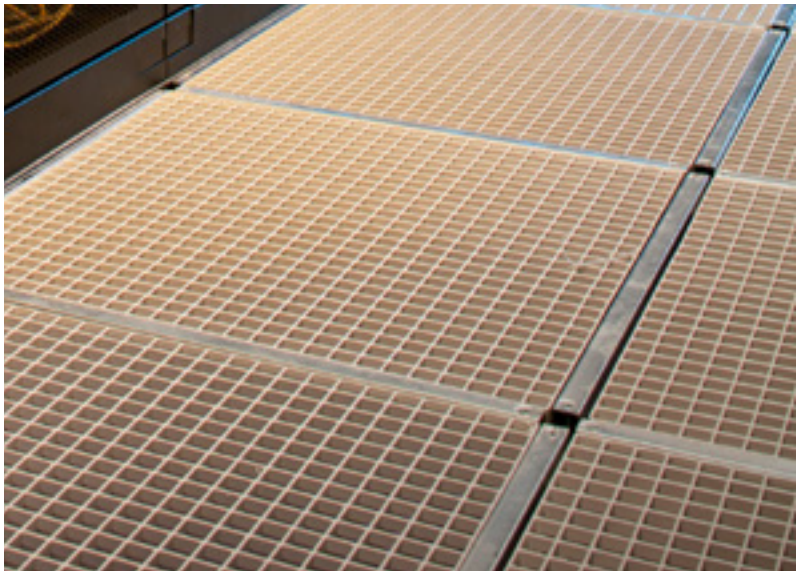
EQUINITI
TOPLEVEL

GOVERNMENTAL COLLABORATION ONLINE:

A QUESTION OF SECURITY

Equiniti Toplevel



Introduction

Online services have revolutionised the way we live and work, driving economic growth and giving us new ways to connect and co-operate with one another. Falling costs mean accessing the internet has become cheaper and easier, allowing more people in the UK and around the world to use it, feeding the flow of innovation and productivity and reducing time to market. The Government Digital by Default programme brings new opportunities but also new threats.

The channel shift of communications between and with governmental teams – away from telephone, postal and face to face interactions and towards online allows for services to be improved, costs to be reduced and staff and resources to be deployed more efficiently. However, in a digital age online communication opens up increased risks of cyber-attacks. In fact, the Annual Global Information Security Survey reports that there has been a 23% increase in losses per security incident in 2014 alone. As cyber criminals continue to develop and advance their techniques, they have also shifted their targets – focusing less on theft of financial data and more on accessing information.

Government bodies are particular targets, and they have high profile and specific responsibility to citizens as well as employees. Reputation and trust are major driving forces and must be protected in this boundary-less environment.

> “The growth of the internet has been the biggest social and technological change of my lifetime. It is a massive force for good in the world in the way it drives growth, reduces barriers to trade, and allows people across the world to communicate and co-operate. At the same time our increasing dependence on cyberspace has brought new risks, risks that key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against. The UK Government takes these risks seriously.”
>
> THE RT HON FRANCIS MAUDE MP, MINISTER OF STATE FOR TRADE (2015-2016)

What's your risk?

Government is unique as a provider of online services to personnel and partner organisations, consumers and citizens. Digital services present a number of risks, from Denial of Service attacks to exposure of consumer data. It is expected that they are private, safe and secure. In response, the UK Government considers cybercrime to be a Tier 1 threat, putting it on a level with international terrorism and major incidents.

There is a natural conflict between security and ease of use in the development process, as digital developers are typically focused on the customer experience, and stringent security can be seen as a barrier to the adoption of new services. This can mean that if security is addressed towards the end of the project lifecycle –sometimes as a retro-fit element – the effort involved in integration can mean a lot of extra time and cost before the product can go to market.

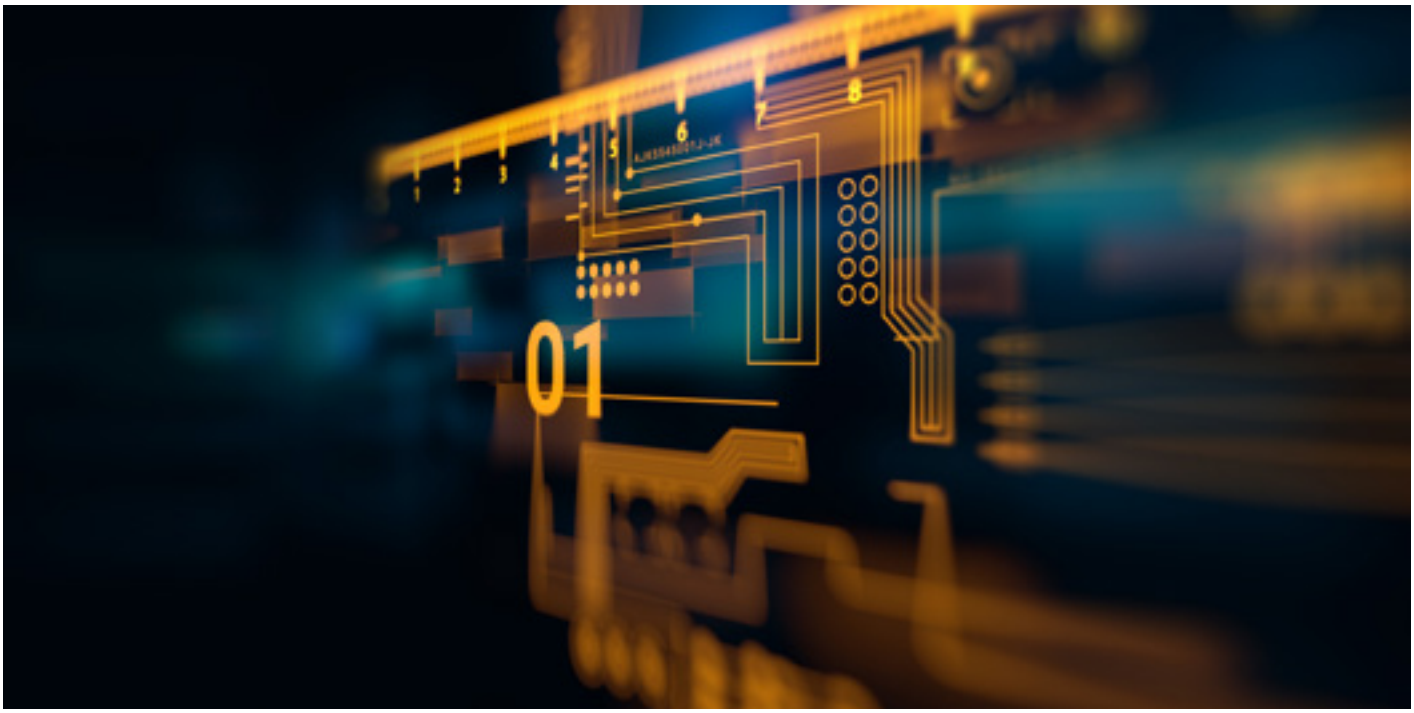
According to the report, 'The Cost of CyberCrime' released by the UK Cabinet Office, the following are key areas that can affect a government body's cost structure:

- Costs in anticipation of cybercrime: Security measures, such as antiviral software installation, cost of insurance and IT security standards maintenance.
- Costs as a consequence of cybercrime: Monetary losses to organisations, such as gaps in business continuity /service availability and losses due to IP theft.
- Costs in response to cybercrime: Paying regulatory fines and compensations to victims of identity theft, and cost associated with investigation of the crime.
- Indirect costs associated with cybercrime: Costs resulting from reputational damage to organisations and loss of confidence in cyber transactions.

Indeed, this last element, around an organisation's reputation is arguably the issue that is uppermost in the mind of a government body, given the responsibilities they hold to the taxpayer.

In the corporate world, the Annual Global Information Security Survey reveals that in the last year, there has been a 75% increase in organisations reporting losses of more than £6million per security incident.

So, how do you embrace the benefits of digital services while at the same time minimising your risks?



Digital security best practice

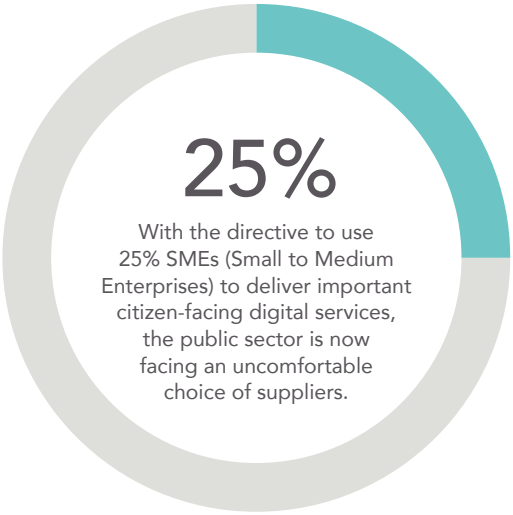
There are a number of ways to ensure the ways you interact online meet the required levels of security as you introduce new digital services, not least looking out for CESG assurance, comprehensive risk assessments in the form of RMADs and, at a fundamental level, adherence to the principles of Cyber Essentials.

Essentially, these things come together to indicate that a service or solution conforms to a set of security requirements, including consideration of:

- AVAILABILITY: all assets, including systems and information, are available to authorised users when needed
- AUTHENTICATION: identify who is using the services (person or software programme)
- AUTHORISATION: give the right people access to the right resources
- CONFIDENTIALITY: prevent unauthorised access to information
- INTEGRITY: prevent information from unauthorised modification, and ensuring that information can be relied upon and is accurate and complete
- TRACEABILITY: chronologically interrelate any transaction to a person or system that performed the action in a way that is verifiable.

Fundamentally, security polices, practices and procedures must be in place as well as ensuring your IT environment is secure, protecting e-Government systems against attack, detecting abnormal activities and having a proven contingency plan in place.

Historically, Government organisations have turned to the larger Systems Integrators (SIs) to take away their pain, manage their projects and to provide inherent peace of mind. With the directive to use 25% SMEs (Small to Medium Enterprises) to deliver important citizen-facing digital services, the public sector is now facing an uncomfortable choice of suppliers. The question resounds: Can these organisations deliver the robust and secure services required of a government organisation?



Not all SMEs are equal

While there are clear benefits to working with SMEs rather than an SI – you're not tied into a long-term contract, you're not paying for over-servicing, projects are delivered much more rapidly – still the doubts continue. We know from a recent UKTech Magazine survey that 33% of civil servants have concerns about SMEs' capabilities to deliver complex projects long term: critical projects involve more than developing some HTML code and creating some forms.

Does a SME and its developers have Security in their DNA? Can they integrate with your complex back end security and data storage systems? Certainly, in some cases this is not the situation.

What to look out for

When embarking on citizen-based digital projects and choosing a supplier, it is useful to bear the following in mind:

- Involve the IT security team on day one of the project
- Look at how sensitive data is protected. For example, what level of security is appropriate for each set of data records?
- What security accreditations do the supplier's security team have?
- Is the solution designed to be OFFICIAL /IL3 compliant?
- Risk Management – Does the organisation you are dealing with use a proven risk management process such as Prince 2?
- Time to market – has your supplier factored in the security review at the end of the project and its effect on project delivery timescales?
- Does the solution have existing in-built plug-ins that allow it to integrate with your firewall and Antivirus systems?
- Once the security solution is developed is it easily repeatable for other deployments?
- Does the organisation you are looking to work with have a track record of security skills and investment beyond self-assessment through (e.g.) the Cyber Essentials programme?
- Does the supplier you are dealing with have a view on addressing common digital threats such as Distributed Denial of Service (DDoS) attacks? (According to an Akami State of the Internet report, there has been a 90% increase in DDoS attacks in Q4 2014 compared to Q4 2013.) Do they regularly have their solutions penetration tested by CLAS consultants?
- Platforms – Do they have a strategy around hardening the hardware platforms? Many attacks aim to disable system hardware thereby crashing the secure software that lies on top.

These areas are fundamental to any project from the start – not least in the Public Sector. This is why we, even as an SME, can meet and surpass the requirements indicated above.

Security built-in

Look out for solutions which deliver Government-strength security 'out-of-the-box', whether installed or hosted. Our products, for example, have security built-in with CLAS level security testing. Our unique architecture allows Government, customers and outside agencies to interact through a single joined-up system that takes into account the complexity of the particular IT environment and data systems in which the services need to operate, integrating with existing security technologies and policies.

Outreach, our Software as a Service (SaaS) platform sits at the heart of a set of pre-built and configurable online applications which facilitate digital interactions between Government personnel and partner organisations, consumers and citizens by delivering government-strength, proven software solutions to reduce the cost, effort and risk of deploying online services. From self-service appointment booking, online form presentation and data collection, service eligibility and application processing to case management, Outreach brings together the benefits of bespoke customer facing applications and integration, with the cost advantages and deployment speed of COTS.

Outreach's in-built security capabilities ensure you meet the best practices described above – from controlling access to sensitive data through to password protection, digital signatures, fine grained access control, one time security codes, white- and black-listing and user auditing as well as single sign on functionality. Architecturally, Outreach provides inbuilt protection from Denial of Service attacks, strong encryption (AES 256), antivirus integration and ISAPI support allowing for dual skinned firewall architectures. With all this "out of the box", it represents a low-risk, quickly deployable option.

Proven security

Outreach has been accredited to IL3 / OFFICIAL Sensitive levels and has delivered solutions to organisations including the Legal Aid Agency and OFSTED.

As many of our customers make use of online web based services, we frequently commission penetration testing and security reporting on their behalf using different CLAS and CHECK approved security firms. Findings are incorporated into our products' R&D, which means that our entire customer community stands to benefit from reuse and continuous improvement through product security upgrades and enhancements.

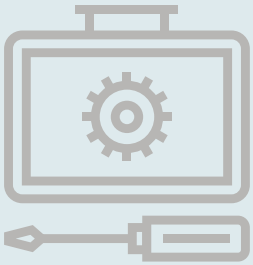
We follow guidelines set out by the Open Web Application Security Project (OWASP), a worldwide not-for-profit charitable organisation focused on improving the security of software. Their mission is to make software security visible, so that individuals and organisations worldwide can make informed decisions about true software security risks.

In addition, and in pursuance of our commitment to be recognised as a low risk partner for Government, we have achieved Pan Government Accreditation (PGA) by CESG, the information security arm of GCHQ, for the handling of OFFICIAL data. This verifies the high level of security assurance provided by our solution and to make it easier for large government departments to procure services in line with the 'Digital by Default' drive mandated by Government.

The certification removes the need for public sector bodies to perform their own time-consuming and costly internal comprehensive risk assessments (RMADs) and to independently assess the security assurances of the provider, helping to make the process of selecting and committing to a solution more straightforward and less time consuming.

The successful completion of the PGA process reduces the risk of an unsuccessful RMAD forcing organisations to re-architect elements of their solutions with the related costs and lost time this would incur. It demonstrates that our platform has been tested to a higher level than self-certification based on Cyber Essentials criteria.

The extensive investment in time and budget in the accreditation process demonstrates our commitment to the delivery of best in breed Government digital solutions in conjunction with our investment in ISO 27001.



The extensive investment in time and budget in the accreditation process demonstrates our commitment to the delivery of best in breed Government digital solutions.

Key deliverables

Information Assurance

Both Toplevel and our datacentre partner are ISO27001 accredited and our services have been used and accredited previously in major HMG departments to host IL3 / OFFICIAL Sensitive information assets. Both Outreach and our Cloud delivery service configuration, which is SQL Server based, have been rigorously security tested and assured. To ensure the security of all Toplevel GCloud Services, Toplevel has worked with CESG Check-approved and other security testers with UK industry accepted certifications and with CLAS consultants, to implement a comprehensive security architecture.

Security testing and risk management are carried out in a way that allows the option for all Government customers accessing our GCloud Services to leverage the benefits of a single protected environment reserved exclusively for them.

Security and Reliability

We operate a scalable, proven security model, with secure n-tier architecture protecting information assets and data flow. A fully resilient hardware solution is provided in the primary datacentre, with no single point of failure. There is also an additional option of fail-over equipment in a secondary datacentre if required.

Systems are configured to give privileged access to Government Staff, enabling them to access appropriate customer data and protecting self-service customers from seeing each other's confidential information.

Proven methodology

Toplevel application development processes adhere to the OWASP guidelines and we operate an ITIL-based service department with responsibility for monitoring and maintaining security levels including maintaining patch levels on operating systems, anti-malware software, applications and devices such as firewalls.

Government-Strength Deployments

We have a policy of obtaining SC Clearance for all Toplevel operational staff and customers can choose to take advantage of our Protect+ virtual private Cloud environment, which is only open to government customers. It employs advanced segregation techniques and increased authentication security for remote support and management.

Our solutions can be configured to meet individual organisations' security needs, including partitioning between hardened web server, application server and database server with firewalls between each partition. As appropriate, we can introduce advanced data encryption techniques.

Conclusion

So, security doesn't need to be a barrier to adopting online services which allow you to be responsive to your stakeholders, cut costs and use time and resources more efficiently and effectively. Neither does it have to be a concern when you're considering which provider to partner with.

We have security at the heart of all we do, while helping you to reduce time to delivery, time to market, improving agility and flexibility and offering peace of mind. And if you still have any doubts, take reassurance in our 52 major deployments across 36 clients, including the Ministry of Justice, Legal Aid Agency, Home Office, Her Majesty's Passport Office, Arts Council England, Heritage Lottery Fund, Ofsted, Commonwealth Scholarship Commission, Creative & Cultural Skills Council and Environment Agency.

We deliver fast, often configuring highly tailored services within a few weeks, and our solutions are proven, high quality, high security government-strength services.

We deliver fast, often configuring highly tailored services within a few weeks, and our solutions are proven, high quality, high security government-strength services.

About Equiniti Toplevel

Toplevel provides end-to-end digital and case management solutions that allow Public Sector organisations and individual case-workers to interact more easily with other departments and the citizens they serve.

We improve customer experience and help staff to do their jobs quicker and better by replacing paper, telephone and face-to-face services with more efficient digital alternatives

EQUINITI
TOPLEVEL

Call us now or use the enquiry form on our website to discuss how we can help you deliver your next project
T: +44 (0)1453 852 700
E: email@equiniti-toplevel.com W: www.equiniti-toplevel.com
500 Stonehouse Park, Stonehouse, Gloucestershire, GL10 3UT