CAPITA

Why risk it?

5 issues surrounding secure localisation management

Capita Translation and Interpreting - **WHITE PAPER**

Big data | Storage | Processes | Users | Technology

Inside the WHITE PAPER

Why the sudden concern over security?

Recent years have seen some significant breaches of cyber security and web vulnerabilities, resulting in some high profile international headlines. Not a week goes by nowadays without a tale of woe befalling some household name, causing us all to sit up and take notice of the state of security in this internet age – even if all we do is change our social media passwords.

As guardians of customer data – in the form of translation content, reference materials, translation memories and the like – how effective is the language industry when it comes to cyber security, and how well do we serve our customers' security needs?

It is fair to say that the general public only get to know about a fraction of the cyber-attacks against organisations that occur almost every hour of every day; attacks perpetrated by a range of different parties, from casual hobby-hackers and 'hacktivists' through to more organised data theft on a grand scale. If this is of no concern to you then perhaps it should be, since most of the governments of G20 countries cite cyber security and the associated risk of data protection and system hacking as a Tier 1 threat, alongside international terrorism and military conflict.

Security and the Internet of Things

It's not just governments that need to take this threat seriously though; we all need to assess our security profiles and maintain effective controls against unauthorised cyber activity, which is no mean feat given that the internet is so tightly woven into the fabric of our businesses and society in general.

The ever-increasing proliferation of internet-connected devices – things that until recently we all considered to be passive, everyday objects – merely adds to the challenge of keeping data secure. True, your IT systems are unlikely to be infiltrated through your toaster, but the recent story of wireless webcams being compromised by the simplest of tweaks (with resulting images being posted for all to see on the internet) serves as a timely reminder that we all need to take steps to protect our data.

Is building a wall enough?

Most of us associate data protection with firewalls, which have been a mainstay of IT security for many years. Indeed, over the millennia, the humble wall has been the method of choice for many who have sought to secure their assets, defending them from external attack. From The Great Wall of China to the Roman fortifications, these fortresses created seemingly impenetrable barriers in an effort to keep out would-be invaders.

In the majority of cases however, such fortifications alone were not enough to save civilisations from their eventual downfall – as those within their confines were lulled into a false sense of security. Feeling safe inside their domains, inhabitants became complacent, forgetting what might happen if their defenses were breached, which inevitably they were.

Breaches generally came in two forms: the first was catastrophic failure, whereby once the mighty wall was scaled no other protection was in place to prevent invasion, whilst the other was more insidious. Over time, strategies of engagement with the outside world gave way to carelessness about who and what was coming in the gates.

Who can we learn from?

If you are beginning to draw parallels with building walls and how the world approaches data security today then you'd be right to do so. However, how much have we actually learned from history? The answer depends on the kind of organisation you ask and the importance they attach to information security, which generally comes down to their reliance on it for their livelihood. Those that act as data controllers or high-volume data processors generally have a very good understanding of what secure means, supported by mature, audit-driven policies and procedures.

Arguably, one of the most effective information security regimes – that can serve as a benchmark for us all – is the Payment Card Industry Data Security Standard (PCI DSS), which helps safeguard the details of approximately 95% of credit cards on the planet. Its implementation goes a long way in ensuring adequate protection against security breaches, by combining the need for physical defenses with compliance-driven processes.

Are there standards for protecting data?

The table below is a summary of the PCI standard that has been generalised to refer only to 'data'. Interestingly, the control objectives and their corresponding requirements still hold true, despite the broadening of the scope. Indeed, any rational person reading this would expect all of their data (not just credit card details) to be handled according to the standards described.

Control Objectives	Standard Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Data	3. Protect stored data 4. Encrypt transmission of data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

So what about the language industry?

Thus far, we have highlighted the need for solid information security controls and identified a good standard that we (hopefully) all agree should be adopted in one form or another. How is it then that some players in the localisation industry appear to be lagging so far behind in espousing appropriate security controls for the data that they process?

With many language service providers being self-employed linguists working out of their homes, it actually fits one definition of a cottage industry very well. But of course we all know that sitting above this talented global network of linguists are the language service companies, who sell the localisation dream and manage its delivery - at local, national and international levels.

Who's responsible?

From individual linguists to language services providers to software manufacturers – we all have to take some responsibility for the situation, and are all going to be involved in fixing it, before it's too late. We can either proactively manage how our industry responds to the threats posed by cyber-crime or we can bury our heads in the sand and pretend the problem doesn't exist. The trouble with the latter approach being that by the time we come up for air, the landscape will have changed and we could be facing an uphill battle to regain trust.

If you are a buyer of language services, you have to play your part as well. Only through your insistence that information security is given the importance it deserves will the industry really start to change.

You have the ability to demand change, the industry has the ability to deliver it.

Are you really clued up on security?

One would imagine that risk-aware organisations will know exactly what happens to their data when they send it to their language service provider. But detailed risk-management isn't the norm. What is, still revolves around transmission of content through unsecure email or unencrypted USB sticks. Without wishing to be too generalist, localisation buyers often appear content to simply sign a non-disclosure agreement with their language service provider, agree to the standard terms and conditions and then assume that their data is secure and well-protected.

However, when there are so many third parties involved in the localisation supply chain how can you be sure that this is the case? How can you know where your data is being sent, who is viewing it, how it is being stored, and whether it is being securely deleted post-project. The maxim of caveat emptor appears to be stretched beyond its practical limits when it comes to the procurement of localisation services.

Whose responsibility is it?

It should be the responsibility of all language service providers to ensure that all parties within their supply chain are security compliant. Translators, proofreaders, DTP suppliers, AV specialists, interpreters, transcribers, language testers – all need to understand the importance of information security and take appropriate steps to conform to documented (and better still, contracted) standards. Similarly, language service providers should ensure that their own staff work to a set of robust information security standards – backed up by regular training and awareness sessions on subjects like the data protection, anti-bribery, fraud awareness and the like.

Technology to the Rescue

Translation Management Systems

Thankfully, the past few years have seen a new breed of translation management systems come to market, which have been designed to address many of the security concerns described above. Making full use of almost ubiquitous access to the internet, their basic premise is to negate the need for file transfers to linguists, meaning that source documents and linguistic assets (translation memories, style-guides, glossaries and other supporting material), remain under the control of the language service provider – typically on their servers.

The products in this space also tend to ensure that linguists only have access to the content they require, and the more advanced solutions offer additional controls - such as non-proliferation and copy/paste lockdown. Role-based permissions also ensure that project managers have restricted system rights so that customer-specific content is only accessible to those who are authorised to work with it. Lastly, in the very best products, all activity is logged as part of a detailed audit trail – enabling language service providers and customers to remain safe in the knowledge that they know who is accessing their content, and when.

A secure environment

However, state-of-the-art translation management systems are only as secure as the environments in which they are deployed. To this end, the hardware, security controls and human processes in place within the hosting data centre play a crucial role in maintaining data security. The use of sophisticated web-application firewalls, perimeter networks, advanced denial-of-service detection algorithms all keep valuable information as secure as possible. When the physical security elements within the data centre are combined with a strong information security management system of the kind imposed by ISO27001 (backed up by regular security audits) language service providers can be sure that they have good control over their data and (more importantly) the data they are trusted with by their clients.

Rise of the Machine

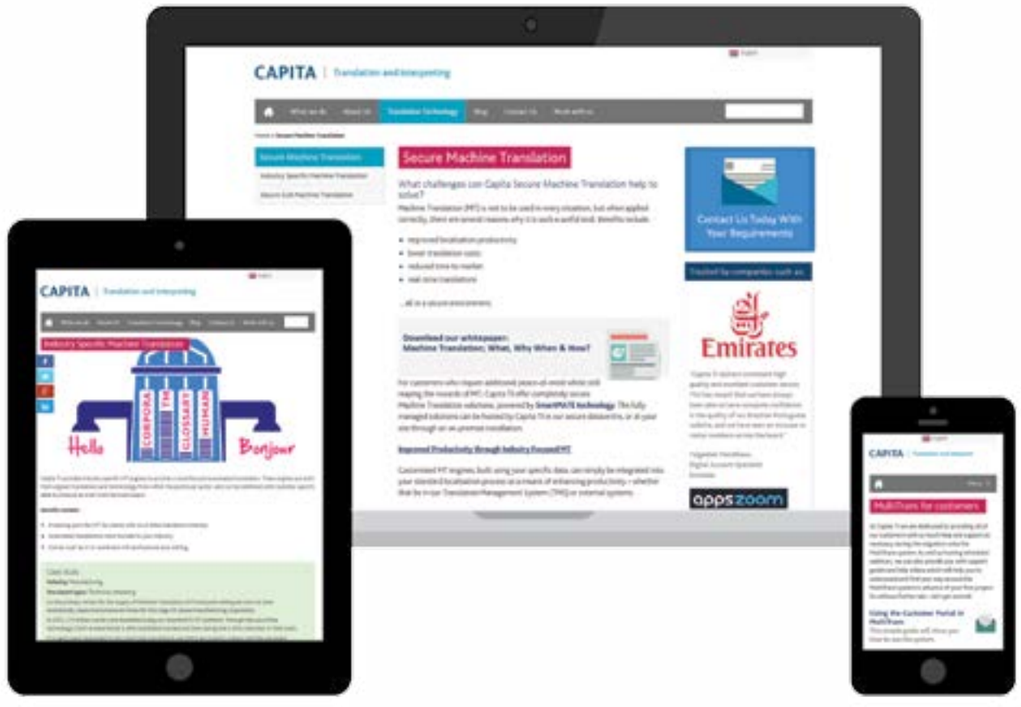
No content on information security would be replete without a mention of free machine translation (the antithesis of professional linguists) and the perceived dangers that accompany it. Amongst risk-averse, highly regulated, international industries there is a growing unease around the use of free machine translation sites by staff wishing to get the gist of content not in their mother tongue. The trend is for such sites to be filtered from use and replaced by private, bespoke machine translation solutions, thus ensuring that risks associated with confidential data loss are minimised – at least through that particular avenue.

Some localisation buyers opt for in-house solutions, whilst others opt for a trustworthy machine translation supplier with the right security credentials who can offer them the kind of assurance they need. Irrespective of the operating model, the scene is set for significant growth in this area of language services as cyber security rises up the board room agenda.

(source: Common Sense Advisory, Why Machine Translation doesn't appeal to some)

Summary

We all need to wake up to the issues around cyber security and start putting in the controls and procedures that will help safeguard our data. While more regulated industries have embraced change and got their 'cyber' house in order, only a few key language service providers, such as Capita TI, have made inroads in this area, offering the kinds of assurance that an increasing number of our customers now demand. We should all now be delivering on our security promises.



F.A.S.T

Capita Translation and Interpreting provides a F.A.S.T. range of language and localisation services:

FAST - In an international industry where dynamic content is the norm, turnaround times for projects can be tight, and customers cannot often predict the volume of work in advance. Our worldwide network of linguists, combined with our innovative technologies and agile workflows ensures we are ideally placed to respond to the need for additional capacity in short time-frames.

ACCURATE - We use linguists that are experienced in translating certain types of content, ensuring your message is accurately conveyed in your target language, protecting you and your brand from any PR or legislative nightmares.

SECURE - We take privacy and confidentiality very seriously, and ensure that your content is protected at all times. All the projects we handle remain under strict privacy guidelines. Our clients trust us implicitly with their work and return to us time after time.

TWENTY-FOUR-SEVEN TRANSLATION SERVICE
As your staff are located worldwide, we understand that requirements may arrive at any time of the day, 365 days a year. Our 24 hour support team based in Manchester is supported by Project Managers in different regions.

Capita Translation and Interpreting

Riverside Court
Huddersfield Road
Delph, Oldham
Greater Manchester
OL3 5FZ
United Kingdom

TEL (UK & EU) +44(0)845 367 7000

www.capitatranslationinterpreting.com