protranslating
A BIG LANGUAGE COMPANY

Visit protranslating.com
Call +1-305-371-7887
Email info@protranslating.com

Spotlight on Security

eBook

eBook

Spotlight on Security

Contents

4 The need to audit people, processes, and technology

5 Remote-working best practices

7 Ring-fencing data with security

9 7 steps to success

Intro

"The rapid switch to remote working in response to the COVID-19 pandemic has exposed companies to shortfalls in their existing IT systems and governance structures and added new vulnerabilities into data and document sharing, communication, and collaborative tools. As the spotlight turns to data security, it is important not to overlook external suppliers when updating security protocols." -Luis de la Vega President, Protranslating.

Before the COVID-19 pandemic, it seemed impossible for many traditionally office-bound workers to imagine that they would be able to work flexibly and remotely from home. Yet, almost overnight, how we work and communicate has changed, placing IT systems and security governance into sharp focus, as companies, employees, and service providers have moved outside tightly controlled on-premises IT environments in response to the need to maintain business continuity in their day-to-day operations.

Not only has this mass migration to remote working exposed both shortfalls and laxity in existing IT systems and processes, but it has also introduced companies to new security threats, including data breaches, phishing, and other forms of cybercrime. From the risk of 'zoom bombing' to the rise in malicious malware and ransomware, the tools, technologies, and communication habits of employees and vendors all need to be considered through a new security-focused lens. But, where should you start?

Measuring the threat

As companies have moved abruptly from their internal IT environments, a whole host of sensitive data – including confidential client information, financial records, legal documents, contracts, and other protected records – have been suddenly transferred onto insecure networks. It is no wonder that high-profile instances of data breaches are on the rise, and new threats such as 'cloud jacking' have emerged.

Companies that have yet to experience a data theft or breach may not have an appreciation for its potential financial ramifications. However, with the average cost of a data breach estimated to be USD 3.86 million, not including long-term damage to trust and reputation, taking a reactive approach to limit exposure is no longer an option.

The implications of a data breach or theft are considerable for all kinds of businesses, but can be even higher for legal and IP (patent) translations. For example, breaking strict protocol for confidentiality in legal transactions or ongoing litigation, and potentially entering trade secrets into the public domain before patents can be secured.

While working remotely offers many benefits for productivity, it exposes companies to greater risk. Security breaches were already on the rise, having increased by 11% since 2018 and 67% since 2014. In the same period, email hacking and hijacking also grew exponentially, with personal emails and mobile phone apps, particularly, at risk. Those numbers increased again during the COVID-19 pandemic, with some sources estimating that cybercrime had risen by a further 600%.

The need to audit people, processes, and technology

The many teleworking, remote meeting, and online file exchange technologies have always raised issues of data security, but the current health crisis has exposed an even greater number of businesses, as employees, partners, and vendors have switched rapidly to working remotely.

In a recent Phishing Attack Trends Report, the Anti-Phishing Working Group (APWG) revealed that the number of phishing attacks reported by its members had doubled throughout the course of 2020. These members include representatives from financial institutions, retailers, ISPs, solutions providers, the law enforcement community, government agencies, university-based researchers, multilateral treaty organizations, and NGOs. Because every employee has access to a company's information assets, that raises the possibility of both intentional employee theft and unintentional damage by an employee targeted by a phishing attack.

It is sobering to note that 90% of data breaches are estimated to occur as a result of employee error – generally a result of falling victim to phishing scams, malware/ransomware, hardware/software misconfiguration, and/or password attacks. The ability of cybercriminals to access sensitive information on otherwise encrypted channels is a growing threat for all businesses, that can cause damage to reputation as well as financial penalties.

According to APWG's research, the financial institution, webmail, and Software-as-a-Service (SaaS) categories were the most frequently hit in the last quarter of 2020, with phishers using an array of deception techniques to fool users. These include domain names chosen to avoid detection, encryption designed to lull victims into a false sense of security, and deceptive email addresses used to spoof trusted companies and business contacts.

In such an environment, protecting a company's information assets is not only the job of the IT department, but should be a priority for all employees, from the board of directors to the most junior member of the team. As with any security protocol, the chain is only as strong as the weakest link, and, therefore, should also be extended to cover all touchpoints, including vendors. Translations should be considered a key part of this IT governance, given the sensitive and demanding nature of the content.

Yet, many companies do not know how their data or documents are being processed, let alone whether – or even how – their internal security protocols are being followed when working with an external translation agency.

Encrypted systems may well be in place when it comes to communicating the brief, but do you know what happens next? Any business that uses contractors also needs to consider where and how they work, from the systems used to share data and documents to the devices on which they access and process the work, and whether or not the data is retained after the project is completed.

Remote-working best practices

By necessity, the language industry was an early adopter of remote and flexible working practices. As Language Service Providers (LSPs) expanded their operations globally, the demand for a multilingual strategy across business and marketing operations increased rapidly, and also expanded to include time-specific and highly confidential legal and IP tasks.

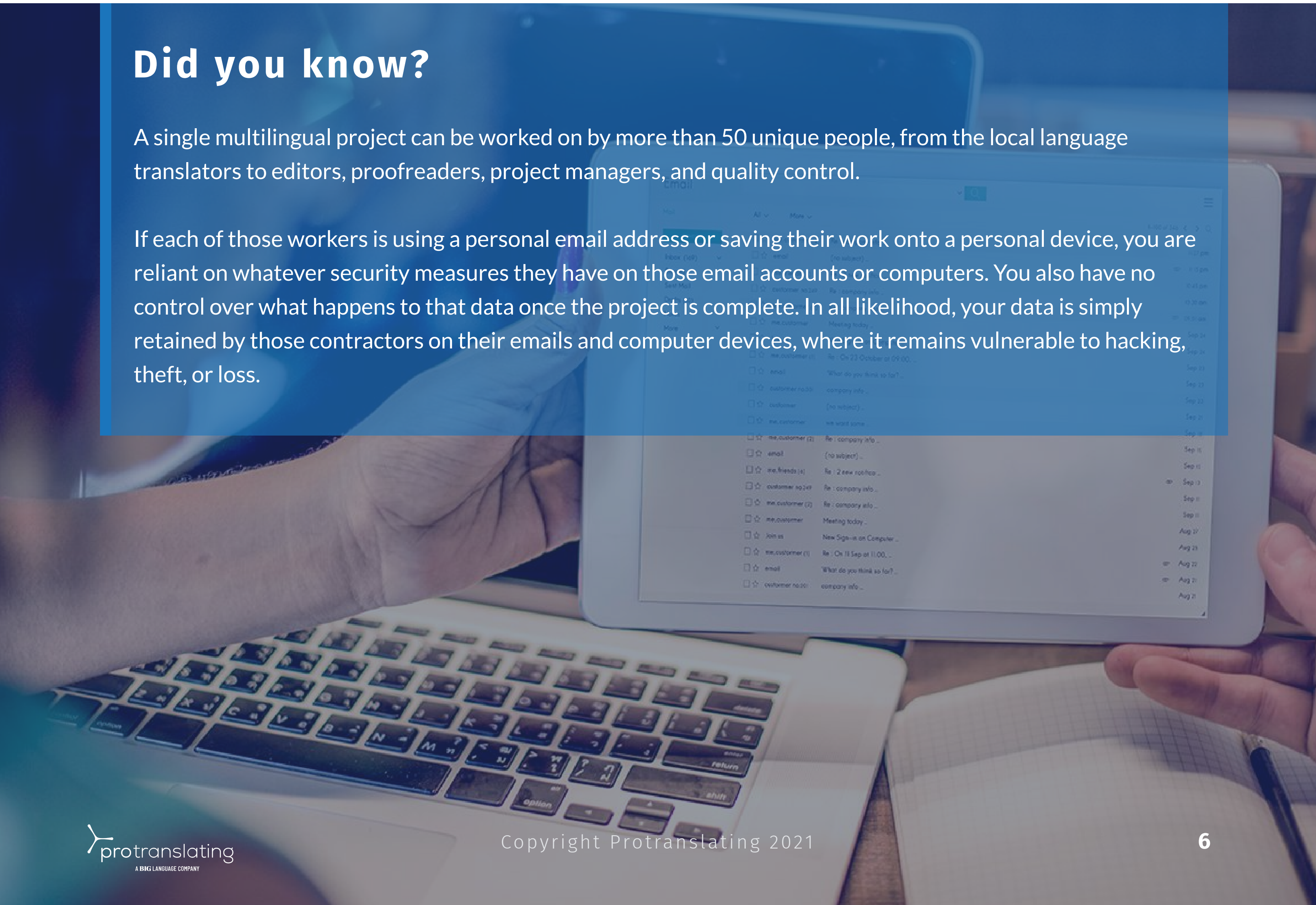
The translation industry that emerged to support these needs operates largely using a network of external linguists, based in different countries and time zones. LSPs provide access to a global network of translators with native speakers covering a wide range of languages and dialects.

As a result of the remote nature of its workforce, the LSP industry has already encountered many of the challenges that other businesses are now facing for the first time. For example, how to protect data when it is in transit and while at rest (e.g., on a translator's laptop), including securing firewalls and networks, encrypting data, authenticating users, and tracking and responding to potential cyber-incidents, all while accommodating high levels of traffic.

But, this is not to say that secure IT infrastructure, devices, and processes are standard across our industry. Unfortunately, the opposite is often true. The number of security gaps in the typical translation process can be very high, as a result of shortfalls in technical and procedural controls throughout the provider's supply chain.

Given the sensitive nature of the corporate and/or legal tasks that LSPs are engaged to deliver, data and process security should be crucial concerns. All too often, however, security is considered secondary to productivity, with confidential and sensitive data routinely shared and stored on insecure personal computers/servers/devices in a range of different countries, including ones with limited security infrastructure, laws, and regulations to protect clients in the case of a data breach.

If companies are to effectively protect their data, they need to include their LSP in their cybersecurity policies, including assessing and controlling how their content is being managed, moved, controlled, and accessed by all members of the translation supply chain.



Did you know?

A single multilingual project can be worked on by more than 50 unique people, from the local language translators to editors, proofreaders, project managers, and quality control.

If each of those workers is using a personal email address or saving their work onto a personal device, you are reliant on whatever security measures they have on those email accounts or computers. You also have no control over what happens to that data once the project is complete. In all likelihood, your data is simply retained by those contractors on their emails and computer devices, where it remains vulnerable to hacking, theft, or loss.

Ring-fencing data with security

The first step is to consider a security audit of that provider's current IT systems and processes. However, in our experience, security audits need to go much deeper to get to the bottom of how data and documents could be compromised internally and externally in a business. Here are some steps we recommend:

- Assessing current procedures for the transfer of data/documents, including how information is stored on devices that do not belong to your company and the use of secure systems and security protocols
- Setting up policies for security measures, including document retention, disaster recovery, and password control, covering employee remote working and also the use of external resources (i.e., outside of your network)
- Centralizing translations through a single end-to-end global supplier to put in place the right technologies and systems to protect sensitive information from a breach
- Choose the right suppliers (i.e., with the right security protocols/certifications in place). This will yield dividends in terms of management of work, improved security infrastructure, and a more security-conscious/trained network of linguists in general

If you are working with vendors that do not have a secure portal and security protocols in place to control communication and collaboration, then you could be exposing private and confidential information to theft or loss. In our industry, for example, that could include a linguist inadvertently exposing sensitive documents by choosing to work from an internet cafe, losing their laptop, or emailing confidential files using a personal account.

The highest standards of security

BIG Language Solutions operates a global network of translators with native speakers covering more than 200 languages and dialects. Given our specific focus on the translation of confidential, legal, and other highly sensitive corporate information, data, and process security have always been key to our DNA.

We take a 360-degree approach to the translation process, looking at the bigger picture to extend security beyond our internal platform so that all touchpoints – people, processes, and technology – are fully secure. Our entire translation approach and IT infrastructure is SOC 2 Type II audited and compliant with ISO 27001 standards for information security management. These standards cover not just the platform, but also our infrastructure, people, processes, and even how we train our staff.

- SOC 2 Type II independent auditing of our internal and external security features provides detailed information about how our clients' data is stored, managed, and used. We are the only LSP with a SOC 2 Type II report that demonstrates our concern for security beyond third-party providers, i.e., our coverage extends beyond the third-party infrastructure that we use;
- In compliance with ISO 27001 standards, we routinely and systematically evaluate security risks, threats, vulnerabilities, and potential impacts to our IT architecture, including network security, malware detection, cloud security, endpoint security, application security, firewalls, data encryption, and secure messaging.

Our translation platform was built around security as the primary driver, not as an afterthought. This means that we can provide clients with unrivaled security and scalability, from guaranteeing data encryption in transit and at rest, to real-time file recovery, protected data availability, controlled and restricted role-based access, customized data retention periods, and continuous vulnerability assessments.

As security threats continue to increase, measures to block ransomware, email hacking, cloud jacking and other forms of cyber attacks and data fraud will become increasingly important. This requires businesses to be proactive in both their internal and external approaches to cybersecurity. Modern businesses need to cover everything – from IT protocols to identifying the channels most at risk of cyberattacks, to educating employees on how to avoid falling for phishing scams.

We believe that language service providers such as ourselves play a key role in establishing a global organization's security posture. Only by providing safe and secure translations to clients can we support a well-rounded approach to cybersecurity, blocking potential breaches at the source, while improving a business's ability to detect a potential threat.

Don't let third-party vendors be the weak link in protecting your customers' data.

Find Out More Here

7 steps to success

How to surround every point your assets touch with security:

Step 1: Assess the Threats

This should begin with an audit of how you manage translations currently, and which suppliers and technologies/tools both you and they use. Watch out for the transfer of your data through highly insecure methods (such as email or insecure FTP sites), storage or processing of data using unauthorized devices (PCs, tablets, personal servers, insecure LSP infrastructure) or tools (online chat, file transfer systems), as well as retention of your documents and data once a project is complete. Documents will often remain stored on personal devices indefinitely because translators and LSPs don't have the policies and infrastructure to support retention policies that automatically or manually ensure the destruction of customer data once a translation process is complete.

Step 2: Look for Vulnerabilities

Processing translations through a portal or machine translation platform is no longer enough. Translation companies are privy to massive amounts of confidential and sensitive corporate/customer data making them prime targets for hackers. It is important, therefore, to extend security beyond the platform to every component of the translation process. By tracking how your LSP manages, transfers and controls access to your content, across all steps in the process, you will be able to identify your exposure to data breach or theft, and assess the security protocols that they have (or do not have) in place to protect you.

Step 3: Vet Your Suppliers

Firstly, check that they have the right security protocols and credentials in place; for example:

- Internal information security policies (ISPs)
- Information security risk assessments
- SOC 2 Type II auditing, ISO 27001 compliance, and HITRUST certification to ensure appropriate information and document safeguarding
- ISO 9001 and 17100 for quality management and industry authentication
- GDPR and CPRA compliance for personal data protection
- PCI DSS for secure payments

Next, verify how recently they have been audited, both internally and externally, and check the credentials of those individuals in charge of handling security. Then, examine the authentication systems they have in place (e.g., 2FA and IP restrictions) to transfer and encrypt content 'at rest, in transit, and in process'. Ask how they ensure the availability of the content, including disruption and disaster recovery measures, in the case of a major disruption. You want to ensure that your documents and data are fully backed up for the life of the project, and that access can be controlled via IP and workstation restrictions for the most sensitive documents (see below).

Step 4: Centralize

Confining content to a single environment (accessible online via a protected user interface) is more efficient, as well as more secure. By setting up a single secure platform for internal and external use, you can minimize threats. Ideally, this should feature a custom-built TMS with open APIs on a security-conscious tech stack. This enables all data, users, and workstations to be logged and audited for every translation task, but also allows for extensive customization where required by a business, as well as automation of common tasks. Minimize the risk of a data breach as a result of unauthorized document retention by working with an LSP that allows you to choose your own retention period for example.

Step 5: Control Access

Control and track who has access to your platform using admin rights/tracking of assets, granular security controls, document recovery, and secure password control. For instance, IP restrictions to authenticate users, hierarchical security settings (password length, password history, password complexity, number of allowed failed login attempts) that match the complexity of your internal security policies; and role-based access controls (RBAC) to assign access to specific teams, departments, and organizations.

Step 6: Classify Content by Risk

Highly sensitive content should benefit from added levels of security; for example, restricting where people work or blocking copying and pasting, if there is a high risk of theft or industrial espionage. Restricted workstations can limit everything from the ability to copy to internet access, and the use of software applications. This helps to ensure there are minimal opportunities for data loss or theft while work is being performed.

Step 7: Apply Global Rules Locally

Embedding corporate governance measures locally will ensure that the platform and its rules are not bypassed, but workflows should also be audited regularly – it is easy to fall back on old patterns, especially when deadlines are tight. Choosing a provider that not only understands the importance of cybersecurity but actively invests in it, can represent the difference between success and failure. If your LSP cannot match your internal standards for security, privacy, confidentiality, compliance availability, and integrity, then now is the time to switch.

Companies, such as law firms, that have yet to experience a data breach may not even be aware of how their sensitive data is being managed or shared, or the potential implications a breach could have for their business.

Take a proactive approach and limit exposure.

Get Started Now

BIG LANGUAGE SOLUTIONS

SECURE. UNIFIED. EFFECTIVE.

Our family of companies includes BIG IP, ISI Language Solutions, Protranslating, Language Link, and DWL bringing a combined 150 years of expertise with offices in 26 cities across the world. Through our portfolio, we customize and deliver language services in more than 240 languages and dialects.