The Importance of **Data Security** in Global Mobility

aires 40th ANNIVERSARY

Keeping sensitive information secure is crucial to conducting business with integrity. Secure websites, data encryption, firewalls, VPNs, and multi-factor authentication are just some of the ways that data is kept secure.

One of the unfortunate realities of modern technology is there will always be harmful actors looking to steal and profit from someone else's information. It seems that no business is completely immune. The lengths that hackers go to in order to obtain information is becoming elaborate and increasingly difficult to thwart and trace. Large corporations, small businesses, non-profits, educational institutions, governments, and private citizens all face daily threats when it comes to data security and privacy. Organizations that relocate employees have equal or greater exposure to these threats.

Employee personally identifiable information (PII) is data that can be used to identify a specific individual. It most commonly includes mailing and email addresses, names, phone, and social security numbers but can also include passport information, IP addresses, login IDs, social media posts, digital images, etc.

Some of this information is shared with global service providers for the purpose of providing support during the relocation or assignment. As such, the global mobility industry creates a massive web of information sharing that must be protected. Any organization relocating employees should be aware of the importance and relevance of data security and privacy and understand the difference between compliance and certification.

Data Security and Data Privacy

Two terms that are heard frequently – data security and data privacy – may seem similar. Although they are related, they address two distinct facets of data handling.

Data security focuses on the processes to protect information (i.e., how it is accessed, how it can be changed). Data privacy focuses on the rights that subjects have to control their information (i.e., how it is used, how long it is stored).

When data is not secure or not kept private and accessed by unauthorized actors, the result is a cyber-attack or breach. Data breaches are something that all companies try to avoid but for which they may be unwittingly targeted.

This white paper outlines what governments have done to protect their citizens' data, what companies can do to ensure they have the proper processes in place to securely handle employee data, and recommendations for how to determine if your suppliers have the ability to securely handle your mobile employees' data.

Legislation to Secure Data and Protect Privacy

Governments have taken action to protect their citizens' data security and privacy rights. Arguably the most significant legislation was passed by the European Union with the General Data Protection Regulation (GDPR). It was put into effect on May 25, 2018. According to www.GDPR.eu, "The GDPR is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU."

The GDPR consists of 11 chapters, 99 articles, and hundreds of pages of specifications that are much further reaching than what is addressed in this document; however, it is critical to know that GDPR consists of technical and operational safeguards that companies must comply with in order to protect personal data. Non-compliance to those safeguards can result in fines.

Another legislation was passed by the state of California in 2018 called the California Consumer Privacy Act (CCPA). This landmark legislation gives consumers more control in how their personal information is collected, shared, stored, or sold.

These are just two examples of how governments have taken control to set standard regulations that organizations must comply with or face consequences.

Compliance Versus Certification

Certification and compliance to a set of standards are both essential when it comes to data security, but the terms are not interchangeable.

Compliance typically entails:

- Adhering to legal, government, and business processes concerning data as defined by consultancy check lists.
- Organizing and managing sensitive data to comply with check lists.
- Protecting personal data and privacy to the best of one's abilities.
- Self-regulating and self-attesting without external audits to ensure ongoing compliance.

Certification goes beyond compliance and generally entails:

- Evaluation of processes by an outside accredited company that determines necessary enhancements to security, maintaining certification, or both.
- Annual audits by an accredited external auditor.
- Significant investment in process development and documentation, which includes departments dedicated to ongoing compliance and maintaining certifications.
- Documented proof that the company has data security and privacy measures in place.

GDPR and CCPA are examples of regulatory standards that require compliance; however, there are additional steps that companies can take to become certified to show they meet rigorous standards beyond what is required by complying to applicable laws.

The International Organization for Standardization (or ISO) is an independent organization that is recognized as a global leader in promoting standards. ISO includes a family of quality standards that are best described as a formula for the best way of doing something. Examples of the standards that commonly impact the global mobility industry include:

- IT security standards that focus on keeping sensitive information secure.
- Quality standards aimed at making work more efficient while reducing possible failures.
- Environmental standards aimed at sustainability - reducing waste and environmental impacts.
- Energy management to reduce energy consumption and the use of natural resources.

Organizations that achieve ISO certification must demonstrate exceptional adherence to strict controls. ISO certifications are not simply a one-time achievement. They are maintained by completing yearly audits.

Certification is not self-regulated as it is with compliance. To be ISO-certified, an organization must be audited by an accredited auditor on an annual basis. There are large investments made to maintain ISO certifications; however, if an audit has any findings demonstrating that standards are not being upheld, corrective actions may be necessary, and certifications may be put at risk.

The Cost of Non-Compliance and Data Breaches

Companies found to be non-compliant with GDPR or CCPA face severe fines. As listed in Article 83(5) of the GDPR regarding severe violations, the fine framework can be up to 20 million euros. The CCPA also imposes fines on violators. The International Association of Privacy Professionals (IAPP) states, "The Attorney General might take civil action, including imposing an injunction and a civil penalty of $2,500 for each violation. If the violation is considered to be intentional then that might rise to $7,500 for each violation." The CCPA figures are imposed per person affected; therefore, if 1,000 consumers are affected, an organization could face a civil penalty of $7.5 million.

For organizations of all sizes, preventing a data breach is necessary to avoid loss of sensitive information, damage to reputation, loss of business opportunities, breach of contract, legal recourse, criminal charges, and fines. In short, data breaches can be costly.

According to "Cost of a Data Breach Report 2020" conducted by the Ponemon Institute and published by IBM Security, the average total cost of a breach to an organization is $3.86 million. The most common information to be compromised in a breach is customer PII records. In fact, 80% of recorded breaches were found to include customer PII.

Given the high percentage of breaches involving customer PII, it is important for all companies to know how secure their suppliers are.

Data Security Standards and Working from Home

Working from home was becoming a more common trend among global corporations before the COVID-19 pandemic and has now become the new normal that is widely expected to continue. With this shift in workplace practices, organizations now more than ever should have basic work from home protocols established, including, but not limited to:

- Company laptops with VPNs, firewalls, and an IP address.
- Companywide training for employee policies and expectations.
- Multi-factor authentication.
- Access controls and active directory.
- Encryption.
- Mobile device management policy.
- Employees must be enrolled and approved to access the cloud.
- Sensitive data only goes to company email addresses, not personal ones.
- Ongoing logging and audits.
- Monthly security awareness training for all employees.

Without these basic protocols, data is at a higher risk and prone to a cyber attack or breach.

Why This Matters in the Global Mobility Industry

Cybersecurity experts agree that companies' supply chains are often their weakest link. This is supported by research from BlueVoyant, which found that 82% of organizations have suffered a data breach in the past 12 months due to a cybersecurity weakness in their supply chain. Breaches within the mobility industry are not unheard of. In the past few months, there have been several phishing attempts to secure real estate proceeds by impersonating an employee through email. Although none resulted in an actual breach to date, hackers will continue to look for the next weak link.

Properly deployed data security through global mobility professionals reduces risks for organizations. By actively becoming aware of their suppliers' competencies with regard to compliance and certification they ensure that they are supporting an approach that extends to the families they move. If data is not properly secured and protected, employees' personally identifiable information, private personnel files, and sensitive business information could be jeopardized.

Privacy standards like the GDPR and CCPA are one step towards compliance. Security certifications such as ISO should be maintained, providing assurance that having gone through the rigorous process of regular external audits that data remains secure as new threats continue to emerge.

Data privacy is just as vital to successful operations as data security. Privacy controls ensure that sensitive data is used properly in accordance with governing laws. When sharing mobile employee data with service providers, it is critical to know that data security measures are in place to protect the data contained within websites, databases, computers, files, and other sources from unauthorized use.

As an industry, global mobility firms collectively strive to create positive and impactful customer experiences for the families that we relocate. As employers and service providers, it is critical to invest tremendous care and attention to safeguarding their information and privacy throughout each stage of the global mobility journey. The risk cannot be avoided, but if it is assessed properly, it is mitigated. Ultimately the goal has to be to enhance customer trust by securing sensitive data.

About Aires

In operation since 1981, Aires is an industry leading, technologically advanced global mobility company. Headquartered in Pittsburgh, PA, Aires has offices across the U.S., as well as offices and legal entities in Hong Kong, London, Singapore, China, Malaysia, and India. Aires' worldwide offices and global partner network extend to 176 countries, ensuring broad coverage for clients. Aires' comprehensive suite of internally built technology tools includes MobilityXchange℠ , featuring application programming interfaces (APIs) for tax, immigration, and HRIS systems. It also includes MobilityX®, custom web portals for both employers and relocating employees offering accessibility to all key data to view, track, manage, and complete mobility tasks and details. Additionally, relocating employees can conveniently access MobilityX® through their mobile devices.

With four decades of industry experience, Aires sets the standard in the global mobility industry, including the highest standards for data security and privacy.

An Industry Leader in Data Security and Privacy

Aires employs an Information Security Management System (ISMS) certified to the ISO 27001:2013 standard. Aires' Privacy Information Management System (PIMS) is certified to the ISO 27701:2019 standard. Aires established credibility in the industry because it was one of the first two organizations in the world to become ISO 27701 certified.

ISO 27701 is the first certifiable international privacy standard. Organizations that receive it have demonstrated exceptional adherence to its strict controls and privacy requirements. To receive certification, Aires underwent a series of rigorous external audits conducted by A-LIGN, an ANAB-accredited auditor. A-LIGN specializes in cyber security, compliance, assessment, cyber risk, and privacy. Among other accolades, A-LIGN is an accredited ISO 27001, ISO 27701, and ISO 22301 certification body. The ISO 27701 PIMS certification complements Aires' ISO 27001 ISMS certification.

Aires' compliance with regulations such as GDPR & CCPA and ISO certifications signal trustworthiness and serve as evidence that data privacy and security measures are continuously met.

Data security and privacy certifications maintained by Aires include:

- ISO 27701:2019 Privacy Information Management System (certified in 2020): Provides management system framework to protect personally identifiable information and demonstrates compliance with privacy regulations. Aires was one of the first two organizations in the world to achieve this standard.
- ISO 27001:2013 Information Security Management System (certified since 2019): Provides a set of standardized requirements for establishing, implementing, operating, monitoring, maintaining, and improving the information security management system.
- Cybersecurity Maturity Model Certification-CMMC (expected certification prior to the 2025 deadline): Unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). CMMC is designed to provide increased assurance to the Department of Defense that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain. All DIB contractors will eventually be required to obtain a CMMC certification by 2025, and Aires is already preparing for this.

Sources

https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

https://gdpr.eu/

https://gdpr-info.eu/issues/fines-penalties/

https://iapp.org/news/a/top-5-operational-impacts-of-cacpa-part-5-penalties-and-enforcementmechanisms/

https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

https://www.ibm.com/security/data-breach

https://www.omnimoving.com/news/aires-achieves-anab-accredited-iso-27701-certification/