Protecting your payroll data during international expansion

As your company's getting ready to enter overseas markets and set up essential services, like payroll, for your new in-country workforce, data security is bound to be chief among your priorities.

To keep client and employee data safe, data privacy and data security are both important. Data privacy focuses on the use and governance of personal data and includes topics such as policies, principles, internal controls and laws about how personal data may be processed, including individuals' rights and protections for cross-border transfers, while data security provides the tools, processes and controls to your organisation's operations to safeguard data. In this article, we'll focus on the changing security landscape that you should consider when preparing to expand your business internationally.

The ever-increasing need for payroll data security?

Personal data that you collect to process your employees' pay is an example of information that must always be properly secured.

Protecting this data both in-country and across borders is now more complex than ever due to the many events that have impacted the world over the past few years. While these events created many challenges, such as an increase in security risks and complex compliance issues, they also provided an opportunity for businesses to expand in ways in which they wouldn't have been able to before.

In response, firms are clearly ramping up their focus on 'infosec' within their payroll strategy. Ninety-nine percent of global payroll leaders say data security has become more important in the last 12 months (and 46% say critically so).[3]

The importance of data security skills within payroll teams

Having **access to advanced digital skills** should be a key component of this strategy, yet current labour market conditions are thwarting multinationals' efforts. According to ISC, "to adequately protect cross-industrial enterprises from increasingly complex modern threats, organisations are trying to fill the worldwide gap of 3.4 million cybersecurity workers."[2]

The real-life impact of this talent shortage can be seen in the responses to ADP's recent global survey, The potential of payroll in 2024. Only 64% of global business leaders say they currently have the data security skill sets they need on their payroll team, with 27% saying they want these skills but lack them.[3]

34%

of firms worldwide said **'continuity of data security protocols'** in payroll processing activities was a specific challenge during their initial response to the COVID-19 pandemic.[1]

60%

of global business leaders say a **security breach has impacted their payroll operation** between 1-5+ times in the last two years.[3]

Download **Guide to safeguarding payroll data in internationally expanding organisations**

Download **ADP Global Payroll: protecting your data as your business grows**

It's clearly critical for firms to establish security best practices for employees, to help prevent the business from experiencing a security incident that could impact payroll. Yet paradoxically, only around half of global business leaders (52%) have developed a playbook and contingency plan **across all their geographies** to protect their payroll operations worldwide in the event of cyberattacks or critical system outages.[3]

There are also signs that data security concerns are stopping companies from moving to a global payroll model, with a shortage of skilled personnel to act in defence. Forty-one percent of large companies cite 'data security concerns' among their top three biggest barriers to implementing a global payroll model across their geographies.[3]

Categories of threats surrounding global payroll data security (Real-time cyber threats)

1 Social engineering and event-based email attacks

- Increasingly sophisticated, this is characterised by emotionally manipulative tactics. Mostly delivered via email, phishing attacks are how most cybercriminals get their toe in the door.
- Messages capitalise on the prevailing context and are designed to elicit emotional responses so that the recipient clicks on the bait.
- A 'business email compromise' (BEC) scam is a highly targeted phishing attack aimed at senior executives and budget holders (designed to encourage the victim to send funds by wire transfer, for example).

2 Acts of ransomware and malware

- Aimed at extorting money from individuals and multiple individuals (e.g., relatives of the victim). Most malware programs are Trojans (malicious software disguised as a legitimate program that can take control of your computer). Backdoor attacks are also on the rise.
- The attacker uses malicious software to block access to a system/steal/encrypt sensitive information and may threaten to release this into the public domain unless a ransom is paid.

3 Data breaches

- These could be from an insider (a current employee) but are usually the result of employee error (sending the wrong file, sending over an insecure channel, sending to unauthorised contact, etc.).

4 Third-party and supply-chain attacks

- This type of attack is on the rise. Criminals target vulnerable links identified within the company's relationship with third-party products, services or information processing facilities.

Companies' differing responses to the threat landscape

Whatever industry your expanding business hails from, as criminals increasingly look to exploit links in inter-sector and international supply chains you'll need to consider the full ecosystem of partners, suppliers and third-party vendors you rely on to service your payroll infrastructure. Cooperation and risk assessments beyond the traditionally technical will be an essential part of any payroll information security strategy in the face of the changing nature of security incidents worldwide.

All types of cyberthreats potentially involve:

- The loss of hugely sensitive employee and financial data
- Penalties for noncompliance
- Compromise of the payroll infrastructure
- Disruption to the payroll process itself
- Distressed employees unable to pay their bills

In extreme cases, businesses could be left unable to pay their staff, causing significant reputational, regulatory and employee engagement challenges.

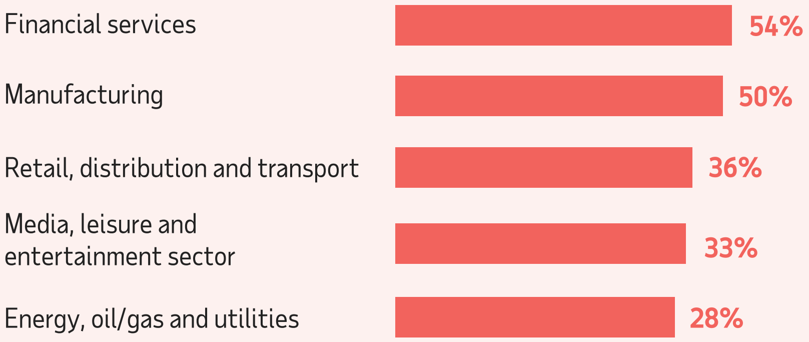
Before your business expands, get the knowledge you need to develop a strong business continuity plan and the resources needed to help protect your business. **Download our guide** to tackling payroll data security issues head-on so that your payroll infrastructure has the resilience to support your business's growth ambitions.

Download our **Guide to safeguarding payroll data in expanding organisations**

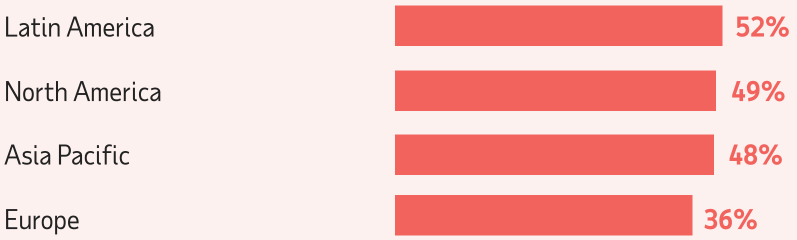
Data on the distribution of cyberattacks in 2022 reveals that the manufacturing sector accounted for the highest share of attacks worldwide (24.8%), followed by finance and insurance at around 19%.[4]

Yet our survey of global payroll managers revealed vastly differing views on the importance of payroll data security across business sectors.

'Payroll data security has become critically important to our company over the last 12 months'



Interestingly, the regional location of the companies surveyed also seems to influence the relative perception of the need to bolster payroll data security protections.



Maintaining the physical security of payroll data in your new market

Expanding companies must also take measures to protect employee payroll data from physical threats — which can be a particular challenge when you're based in another geography. Physical safeguards include the security of work premises and facilities, equipment such as workstations and devices, as well as managing and disposing of physical media containing payroll data in transit.

If you manage payroll in-house, your team will need to implement controls to protect against physical threats and possible outages, as well as safeguard supporting facilities (including elements like electrical supply and cabling infrastructure). Additionally, if your company takes a 'Bring Your Own Device' (BYOD) approach, allowing staff to use their personal laptops, phones and tablets for work purposes, you'll need to ensure your payroll information won't be jeopardised as a result.

1. ADP, The potential of payroll: Global payroll survey 2021.
2. The (ISC)^2 2022 Cybersecurity Workforce Study.
3. ADP, The potential of payroll in 2024: Global payroll survey.
4. Statista, Distribution of cyber attacks across worldwide industries in 2022.

DISCLAIMER: This document and the information contained herein are for informational purposes only. They should not be interpreted as advice, including legal or technical advice to take or to refrain from taking any particular action or to make or not make any decision, including but not limited to any administrative, technical or physical controls, or any hiring decisions.