

Introduction to Payroll Data Security

www.irisglobal.com

IRIS

If there's ever a prime target for criminals, it's payroll.

Payroll data is gold for hackers, fraudsters, and other bad actors who want to extort and disrupt businesses. One successful data breach can yield thousands of identifying details, bank account numbers, salary figures, and other confidential information.



The risks payroll managers face every day

It doesn't matter if you're a business doing your payroll, a CPA firm offering this as a service, or a dedicated payroll bureau; if your payroll system is hacked, it spells disaster.

The direct theft of money is just the start. In the long term, you pay the price with more expensive insurance, potential legal fees, and compensation payouts.

In the meantime, each employee record in your payroll represents an actual human being now vulnerable to identity theft. Their details could potentially be handed over for cash on the dark web.

Any faith you have built in your business will take a serious hit.

But one way or another, you still have to do payroll

You can't avoid payroll if you have staff. The people who work for you have to be paid, and they have to be paid on time; you can't delay this process without an excellent reason.

Likewise, your clients will want someone to do their payroll. If they can't bring it to you, they will look elsewhere.

So, how do you ensure that your system pays everyone on time and keeps their information safe?

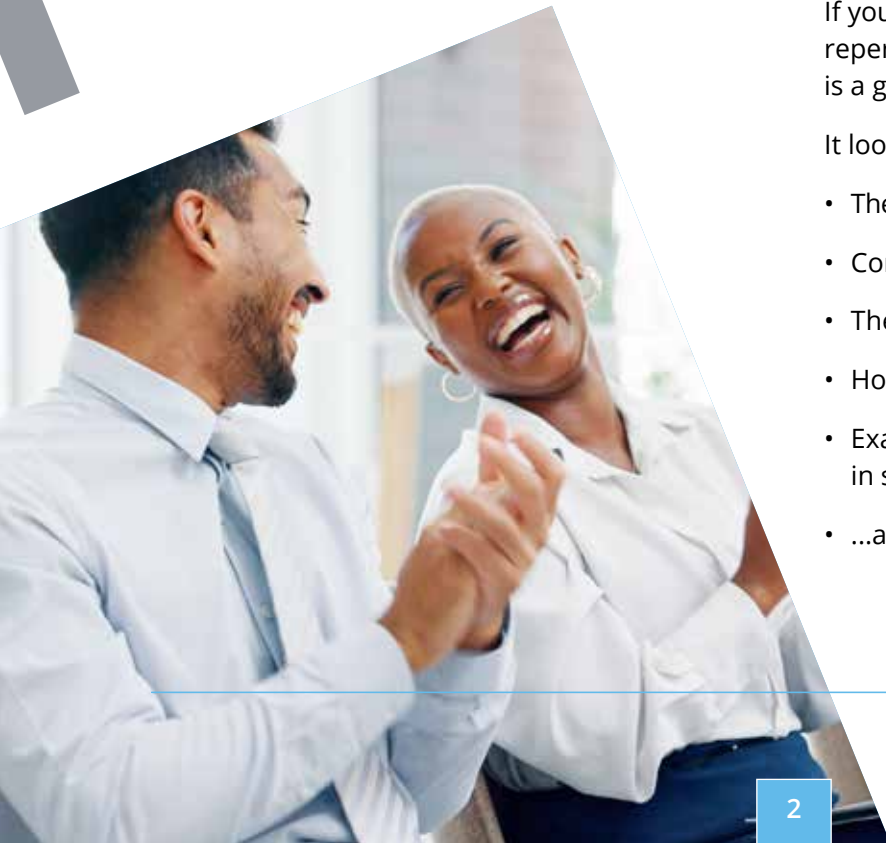
The answer involves both your systems and the people that run them.

About this guide

If you have ever wanted to avoid the repercussions of a data breach, then this guide is a great place to start.

It looks at:

- The threats payroll management operations face
- Compliance requirements
- The best practices for payroll security
- How you can create an incident response plan
- Examples of great data security processes in software
- ...and much more.



Types of threats

Let's review the rogue gallery of threats that jeopardize payroll every day. Here are some situations that can happen to you.

Your system is hacked: Sometimes, a hacker will exploit software that is outdated or has design flaws. Once they get in, a bad actor can steal data or alter it if the goal is disruption.

Your staff falls prey to phishing attacks: When you can't hack software via its weaknesses, people are the alternative. That's where phishing comes in.

Phishing has developed into an art form, with scammers knowing how to trick, manipulate, and pressure people into parting with login credentials or other highly sensitive information.

Most often, it's by impersonating someone you know (like a manager) and creating a sense of impending urgency.

The hacker hopes their victim will react and share data before they realize what's happening.

Thieves in your organization: Not all threats come from outside an organization. Unfortunately, people in a position of trust will sometimes commit fraud. In your payroll, they might create "ghost employees" to siphon money into their account using the name of someone who left or didn't exist. They could also alter data to inflate their wages or even tamper with systems. They might "buddy punch" for fellow workers to cover up absences. We have a whole guide dedicated to fraud, which you can read [here](#).

Malware finds its way into your software:

When hackers breach your system, the potential pain can be multiplied if they deploy malware. Malware includes hard-to-spot, harmful software like viruses, worms, trojan horses, ransomware, and spyware.

All are designed to compromise your business and give hackers financial gain by gathering sensitive information that can be used or sold.

But malware doesn't always need to be added to your software by the hacker that uses it. It's also possible someone in your organization will

download it mistakenly from a website, an email attachment, or a USB drive.

You get held to ransom: Ransomware is a type of malware worth discussing in its own right. Once on your system, malware can encrypt data, rendering it inaccessible until a ransom is paid to the hacker or hacking group. This can paralyze payroll operations, delay payments, and cause financial and reputational damage.

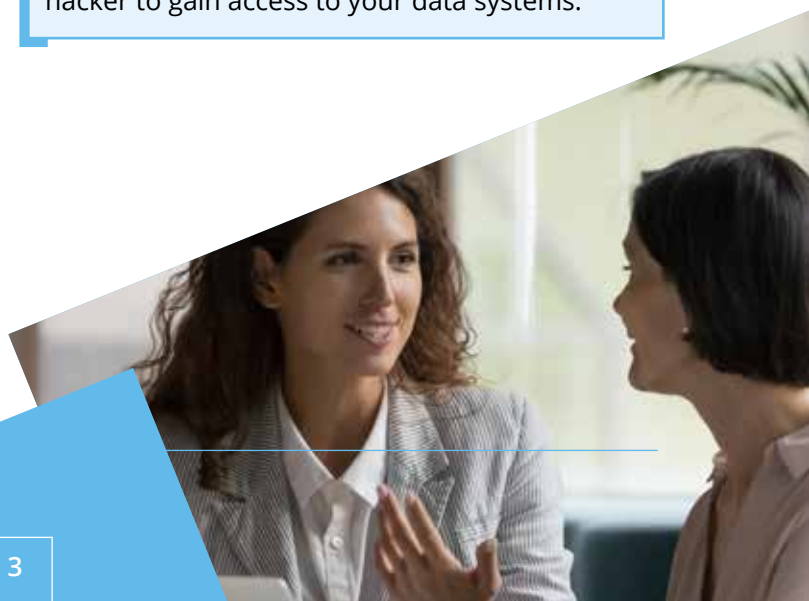
Worse, complying with their demands does not guarantee hackers will release the data.

Phishing is very powerful. Just when you think you know how to spot a scam email or phone call, hackers come up with clever new methods, which now include using AI to replicate people's voices.

Security breaches have seen several major organizations being targeted simultaneously by ransomware before the door gets closed to hackers. One example saw 100,000 people's payroll details being stolen.

The move to working from home has given cybercriminals new opportunities.

Consider hiring a reputable third party to assess your company's security level and get recommendations to improve. The assessment should include, at a minimum, a penetration (PEN) test, which is an authorized simulated cyber attack on a computer system. This test can help determine how easy it would be for a hacker to gain access to your data systems.





Data security compliance requirements

What laws, standards and regulations encourage good data security? Here are a few.

General Data Protection Regulation (GDPR):

Although an EU rule, GDPR significantly impacts US companies handling EU residents' data. It requires strict data protection measures, such as clear consent for data processing, data accuracy, and security.

Health Insurance Portability and

Accountability Act (HIPAA): HIPAA is relevant to companies that handle health benefits data. This US legislation requires the protection of individuals' medical records and other personal health information.

State-specific legislation: Many states have their own laws for protecting data. For instance, California has the Consumer Privacy Act (CCPA), New York has the SHIELD Act, and Virginia has the Consumer Data Protection Act. These laws cover safeguarding personal information, people's rights to access and control their data, and rules for how businesses handle data.

Sector-specific regulations: Other regulatory frameworks might be relevant depending on the nature of the business. For instance, the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act, imposes data protection requirements on financial institutions, which can include certain payroll service providers.

International standards: Achieving global standards like ISO/IEC 27001 (or just ISO 27001) is an evidence-based way for businesses to protect payroll data. The core of ISO 27001 involves a risk management process that requires organizations to identify, analyze, and address their information security risks. It prescribes controls and sets out guidelines for their implementation.



Best practices in payroll data security

We've seen the threats to payroll data security, and we've understood the standards and laws designed to safeguard it. Now it's time to explore some strategies that can help ensure your payroll data stays secure and confidential.

Access control: If you had a high-security building, only the most trusted (and relevant) people would get a key. The same is true with payroll; ensure that only the right people can access your system.

Encryption: Encryption plays a critical role in protecting data within your system and when it is being shared. Even if someone intercepts the data, only the intended recipient has the key.

Two-Factor Authentication (2FA): This is used for signing into software. Businesses often require two-factor authentication as a standard when buying software, and there's a good reason for this. Even if someone manages to guess someone's password, with 2FA, they still need a second form of verification to access your systems. This second form of verification will only be sent to the authorized user (often via text, email or a dedicated app).

Portals, not emails: If you're managing someone's payroll, make sure you update all information using dedicated, encrypted portals. Emails and attachments are less secure; normally, the 'sent' items in an email system are easy prey should systems get hacked. Likewise, if someone asks for information using email and you use a portal, that's an instant warning they might not be who they say they are.

Client screening: Clients can be a risk, so ensure everything is on the level. This includes the business being properly registered and checking all staff have social security numbers. Get to know them as a client before formally putting them on your system; have a security checklist and use it every time.

Client communication: Make sure that when staff leave, the client takes them off the system and that relevant parties are notified when a new entry is created. This stops staff from creating fake employees or diverting funds using the identity of those who have left.

Regular audits and monitoring: Regular audits and continuous monitoring allow you to see what's happening in real time and review past activities. This helps quickly identify any unusual actions that could indicate a security breach, ensuring you can respond swiftly to mitigate potential damage.

Keep the environment tidy: To keep data safe, employees should follow strict rules when taking work computers and important information outside the office. Work areas should also stay neat, especially regarding confidential company, client, and employee data.

Use shredding, locking up, or encrypting to protect paper-based information.

Devices and software: Work should only be done on work devices or using devices that have some form of authorization from the business. The same goes for software; keep business data out of personal accounts.

Have guidance and policy: Create a written document outlining security practices, including data access, password management, and incident responses for the relevant staff.

Employee training: Your employees are your primary defense against cyber threats, so they need to learn about any threats specific to your business. Training helps them spot phishing, secure personal devices for work, and grasp the importance of data security. Think of it as giving your team the tools to safeguard the company and themselves.

Make sure, as part of this, they are aware of your policies.

Client training: It's not just your staff that needs to be aware of the risks payroll faces, but clients, should you be managing payroll on their behalf.

Think about having someone formally oversee security; with ownership comes a sense of duty and accountability. Depending on the size of your organization, you could think about hiring a dedicated, trained professional in this area.

Phishing - payroll data security dos and don'ts

The following will help you handle thieves posing as employees, clients, authorities and more.

- If an email seems suspicious, avoid clicking on links or opening attachments.
- Avoid using email to send important information like social security numbers, bank details, or tax ID numbers. Before you hit send, check that your attachments don't contain any private data.
- Avoid responding to requests for personal information through email, phone, or text. Use a secure platform for submitting such data.
- When checking an email, pay close attention to the email address or domain name, not just the sender or display name. Watch out for spelling mistakes, as they could signal that the email isn't from the expected source.
- Don't assume you know who an email has come from; even if you know the email address, you can't be sure the email account hasn't been hacked. Instead, opt for an extra way to verify an email comes from the person it claims it has.
- When you get a request for information that seems legitimate, be sure to contact the company using confirmed contact details (not just the ones in the message).

Spotting thieves in your organization

How do you spot thieves in your organization?

When they steal money, that money often begins to show in their lifestyle. They might exhibit changes in their spending habits that don't match their salary. Maybe they are going on luxury vacations, wearing new designer clothes, or purchasing a flash car.

And they will want to cover their tracks. This might reveal itself when they work long or irregular hours. They might be unwilling to take a vacation, and they will come into the office when ill rather than take sick leave.

Of course, be careful. Some of these behaviors can point to other situations. For instance, their spending might be thanks to having a wealthy friend, relative or partner.

Software and data security

The right technology can make all the difference to your payroll data security, but what are you looking for when you choose a solution?

Payroll management systems: key features

A robust payroll management system is the backbone of effective payroll processing and management. At its core, such a system should offer built-in encryption to protect sensitive data regardless of whether it is on your system or being shared with a client.

It's also very important to see audit trails. Audit trails provide a detailed record of all transactions and changes within the system, enabling administrators to track any adjustments made to payroll data. This helps identify potential discrepancies or fraudulent activities.

Software built for the cloud (cloud-native) is also built to protect against hacks, thwarting bad actors at every turn.

To bolster your payroll data security, make sure your computers have antivirus, anti-malware, and firewall solutions.





A working example: the IRIS approach to software security

When you use IRIS for your payroll solutions, everything is protected by layers of watertight security.

First, everything we do is cloud-based, meaning that all the issues with vulnerable desktop software are no longer an issue. For example, you don't have to wait on updates anymore, and the dangers that come with locally stored (so easily stolen) data are a thing of the past.

Instead, everything is protected on servers held by Amazon Web Services. AWS is a server infrastructure built for speed and end-to-end security and is known for having the largest market share when it comes to cloud infrastructure.

Keeping a close eye on traffic

Databases are kept separate, and access is tightly controlled, with only the right people having the right access to the encrypted data.

To get in, they have to have two-factor authorization as standard. Even the passwords people use are encrypted so that no hacker ever has a chance of stealing them (as long as your firm follows best practices!).

Behind the scenes, all traffic is closely monitored. The slightest change from the norm is enough for IRIS to go on alert and check that everything is safe.

Being prepared: your incident response plan for payroll data breaches

You need to prepare should the worst happen. So, how do you go about this?

1. Preparation is key: Start by putting together an incident response team. Make sure you do this before anything happens. Each member should have clear duties; the team needs IT experts, legal advisors, HR staff, and communication specialists. Ensure everyone understands their role if a breach occurs.
2. Detection and analysis: It's important to have systems to spot irregularities and alert you to breaches early. Doing so affects how much damage an attack can do.
3. Containment and eradication: Swiftly focus on containment upon detecting a breach. Disable impacted accounts, alter passwords, and isolate compromised systems to thwart additional unauthorized access. Next, tackle the leading cause of the breach, such as malware or a security weakness.
4. Recovery: Once it's safe, restore affected systems from backups. Ensure all systems are clean before bringing them back online. You might also implement additional security measures to prevent future breaches. Afterward, communicate with stakeholders about what happened, how you resolved the situation, and any new measures to prevent future attacks.
5. Post-incident analysis: It's time to learn from experience. Examine how the breach happened and how you reacted. What went right? What could have gone better?

Prep for everything. Hackers are one threat to your data security, but natural disasters are another.

Legal and PR considerations

As suggested in steps one and four above, running parallel with the data breach itself are legal and public-facing ramifications.

You need to know which regulatory bodies need to be informed and what information needs to be disclosed. In the U.S., this may vary by state.

How you communicate about a breach can significantly impact your company's reputation. Prepare a communication strategy that includes timely, transparent, and factual updates. Empathy and a commitment to taking corrective action go a long way in restoring trust.

Both these spheres require a specialist who can help. If in doubt, don't deal with this alone; hire lawyers and public relations specialists who tackle situations like this all the time.

Avoid risk with IRIS solutions

Let's look at how IRIS Payroll Solutions can be a cornerstone for businesses aiming to safeguard their processes.

Outsourcing for national and international business

Managed Payroll Services by IRIS lifts the burden of payroll from your firm.

That way, you can help clients with this daunting task and use the time and effort saved to deliver more value to their business.

For the US and beyond

In today's connected world, growing businesses need smooth, global payroll services.

IRIS handles all the details that give businesses a headache: ensuring they comply with tax laws and securely distributing payments in 127 currencies throughout more than 135 countries. You can pay in USD while we manage the rest, all with the help of a dedicated payroll manager and ultra-secure portals.



Find out more about IRIS Fully Managed Payroll (FMP) services

Software that makes payroll data security simple

It's time to build profitability while reducing workload - IRIS automates the complex, time-consuming tasks that traditionally weigh down your payroll processes.

But IRIS software doesn't just help you with payroll; it delivers a complete, customizable Human Capital Management (HCM) suite that caters to HR and payroll needs.

Enjoy the features, support, and scalability needed to thrive in a landscape where the right tools make all the difference.



Speak to IRIS to find out more

