Bright

Simply brilliant software

Payroll security 101: **Identifying threats and securing your data**

Introduction

In today's digital age, payroll systems are increasingly becoming targets for cyber threats and data breaches. Protecting sensitive payroll information is paramount, yet many organisations find themselves vulnerable to sophisticated cyber threats and human errors that compromise their data security. This guide is designed to arm payroll professionals with the knowledge to fortify their defences against cyber threats.

We will begin by understanding the fundamentals of cybersecurity and its importance in safeguarding payroll systems. Next, we will explore the common vulnerabilities in payroll systems and the impact of human error on data security. We will also delve into the potential repercussions of a payroll data breach, including financial losses and reputational damage. Additionally, you will discover actionable steps to enhance the security of your payroll systems and protect sensitive information. Finally, we will examine how leveraging cloud payroll software like BrightPay can bolster your cybersecurity measures and provide added peace of mind.

What is cybersecurity?

Cybersecurity is like having a digital guard that protects your computer, smartphone, and other devices connected to the Internet from unauthorised users.

Just like a lock on your front door that helps keep burglars out of your house, cybersecurity measures keep hackers and cybercriminals from stealing or damaging your personal information, such as emails, bank details, and passwords.

Cybersecurity includes a combination of software tools, like antivirus programs and firewalls, as well as smart online habits, such as strong passwords and being cautious about what links you click on. These tools and tactics help to create a protective barrier against various online threats.

So, while you're busy running your practice, cybersecurity works quietly in the background to ensure your business's digital presence is safe and secure.

How is your payroll vulnerable to cybersecurity threats?

The risk of cybersecurity threats to payroll data comes from several sources. We've created the following list to show you how your payroll could be exposed to these risks.

Cybersecurity threats

Phishing scams: Payroll departments often deal with sensitive employee information and financial transactions, making them prime targets for phishing attacks. This is where attackers use deceptive emails or messages to trick payroll processors into disclosing login credentials or executing unauthorised transactions.

Ransomware attacks: Cybercriminals may target payroll systems with ransomware, encrypting critical data and demanding a ransom for its release. Given the importance of timely payroll processing, businesses or accountants might feel pressured to pay the ransom to restore their data.

Exploitation of software vulnerabilities: Payroll software that is not regularly updated may contain security vulnerabilities that hackers can exploit to gain access to sensitive payroll data.

Human error risks

Incorrect settings: If payroll software isn't set up correctly, it can accidentally leak sensitive information. For instance, if the user settings aren't strict enough, employees who shouldn't have access might be able to see or change payroll details.

Accidental data exposure: Employees may accidentally send payroll information to the wrong recipient via email or leave sensitive documents unsecured, leading to potential data breaches. And when you are sharing payslips with employees via email each pay period, it could be quite easy to send a payslip to the wrong person.

Poor password practices: The use of weak passwords or the reuse of passwords across multiple systems can make it easier for attackers to gain unauthorised access to payroll systems.

Lack of awareness or training: Employees who are not adequately trained on cybersecurity best practices or the importance of protecting payroll data might inadvertently contribute to security breaches through negligent actions.

What are the consequences?

When payroll data is leaked or lost, the consequences can be severe and far-reaching, affecting accountants, payroll processors, employers, and employees in various ways.

Consequences for accountants and payroll bureaus:

1. **Professional reputation damage:** A data breach can severely tarnish the reputation of payroll professionals. Restoring trust with clients and employees after a breach can be challenging and time-consuming.
2. **Legal and financial consequences:** If found negligent, you could face legal actions, fines, and penalties, especially if the breach violates GDPR.
3. **Increased costs:** Dealing with the aftermath of a data breach often involves significant costs, including forensic investigations, enhanced security measures, and possibly compensating affected parties.
4. **Loss of business:** Clients may choose to terminate their contracts and seek services from other providers who are perceived as more secure.

Consequences for employers:

1. **Financial losses:** Beyond potential fines for regulatory non-compliance, employers may face lawsuits from affected employees or have to offer credit monitoring services to mitigate the damage caused by the breach.
2. **Operational disruptions:** A significant data breach can disrupt payroll operations, potentially delaying salary payments and causing operational chaos.
3. **Damage to the brand:** A breach can damage an employer's brand, affecting their ability to attract and retain talent. Employees want to work for companies that protect their personal information.
4. **Increased security costs:** In response to a breach, employers will likely need to invest in improved security systems, training, and possibly external consultants, increasing operational costs.

Consequences for employees:

1. **Identity theft and financial fraud:** The leakage of sensitive personal and financial information puts employees at risk of identity theft, financial fraud, and unauthorised transactions.
2. **Privacy violations:** Employees expect their personal information to be handled with confidentiality. A breach can lead to feelings of violation and mistrust towards the employer.
3. **Stress and anxiety:** Dealing with the aftermath of a data breach, such as securing bank accounts and monitoring credit reports, can be stressful and time-consuming for employees.
4. **Potential financial losses:** In cases where financial fraud is successful, employees may face immediate financial losses, although these may eventually be rectified, it can still cause problems such as a missed mortgage payment for example.

What can be done to mitigate the threats?

To mitigate the risk of data loss or threats to sensitive payroll data, accountants and businesses can implement a multifaceted approach that encompasses technological solutions, policies, and employee training. Here are key strategies to consider:

Implement strong access controls

1. **Use multi-factor authentication:** Adding an extra layer of security beyond just passwords helps protect against unauthorised access.
2. **Limit access to payroll data on a need-to-know basis:** Ensure that only employees who need access to payroll data to perform their job functions can access it.
3. **Regularly review access permissions:** Audit who has access to payroll systems and data regularly and adjust permissions as roles change within the organisation.

Secure data transmission and storage

1. **Encrypt data:** Use encryption for data at rest and in transit. This makes the data unreadable to unauthorised users.
2. **Secure backup procedures:** Regularly back up payroll data using secure methods to ensure that it can be restored in the event of a data loss incident.

Maintain up-to-date systems

1. **Update your software:** Regularly update payroll systems and any related software to patch vulnerabilities that could be exploited by cyber attackers.
2. **Use reputable payroll software:** Choose payroll software from a reputable provider who are known for their commitment to security and compliance.

Foster a culture of security awareness

1. **Employee training:** Train employees on cybersecurity best practices, recognising phishing attempts, and the importance of reporting suspicious activities.
2. **Establish clear policies:** Develop and enforce policies covering password management, handling of sensitive data, and response protocols for suspected data breaches.

Plan for incident response

1. **Develop an incident response plan:** Have a clear plan in place that outlines steps to take in the event of a data breach, including notification procedures for affected individuals and regulatory bodies.
2. **Regular testing and drills:** Conduct regular drills to ensure that the incident response team is prepared to act quickly and effectively in the event of a data breach.

Legal compliance and best practices

1. **Stay informed about regulatory requirements:** Ensure compliance with laws and regulations related to GDPR.
2. **Cybersecurity insurance:** Consider obtaining cybersecurity insurance to mitigate financial losses in the event of a cyberattack or data breach.

By implementing these measures, accountants and businesses can significantly reduce the risk of data loss or security threats to sensitive payroll data. It's important to continuously evaluate and update security practices in response to evolving cyber threats and changes in the business environment.

How cloud payroll software, BrightPay, can help

Cloud payroll software, when chosen carefully and used correctly, can address many of the points related to mitigating the risk of data loss or threats to sensitive payroll data. To give you an idea of how cloud software can help, here are some of the features which our own cloud payroll solution, BrightPay, has that can help keep your data safe and secure, and lower the risk of cybersecurity threats:

Implement strong access controls

User permission settings: With BrightPay, you have full control over who has access to what data. There are four types of user permissions that you can set in BrightPay, and they all have different capabilities. The different users are owner, administrator, payroll processor and billing manager. The owner is the user who has full control over the payroll software. The administrator will have similar access to the owner, but they won't be able to remove the owner as an administrator. The 'payroll processor' user will only be able to access the payroll. The billing manager will have access to the billing section only and be able to do things like see invoices and update any billing details.

Say for example, you don't want payroll processors to have access to your own company's payroll. You can mark an employer file as "admin only" and then only the administrator will have access.

Sign out everywhere: To start using BrightPay, you need to create a Bright ID. Bright ID is an online platform from where Bright customers can manage things like their licences, billing and security. You will also use your Bright ID login credentials to access BrightPay. For a complete security reset, from the Bright ID platform, you can click a button to sign out from everywhere that your Bright ID is in use. This means that any browser or device that was signed in to BrightPay will have its access revoked and will require signing in again to continue.

Secure data transmission and storage

Data hosting: BrightPay securely hosts its data on a remote server instead of storing it on your local desktop, ensuring optimal security measures are in place to protect it. BrightPay utilises the cloud computing service Microsoft Azure to store users' data, which is one of the leading file hosting services in the industry.

Automated backups: BrightPay takes your security measures up a notch by continuously backing up your payroll data, while you work. This means no more having to worry about your payroll data getting corrupted or lost, it's safely stored in the cloud.

Employee payslips and documents distribution: Emailing payslips can be risky when it comes to GDPR, as you could easily send the wrong payslip to the wrong person. With BrightPay, payslips and other payroll documents such as P11Ds and P60s, can be made automatically available to employees through BrightPay's Employee Self-Service portal. This enhances security and lessens the risk of sensitive payroll information being shared with the wrong people.

Integrations with other software: Integrated tools for accountants not only streamline the workflow and enhance efficiency but also play a crucial role in improving data security. When accounting tools are integrated, data can be transferred seamlessly between systems without the need for manual entry or sending files through less secure means like email.

Maintain up-to-date systems

Automatic Updates: BrightPay automatically updates to the latest version, eliminating the need for manual downloads. This keeps the software secure with the latest security enhancements.

Foster a culture of security awareness

User activity monitoring: With BrightPay, multiple users can access and work on the same payroll file, at the same time. When in the payroll, you'll be able to see who else is in the payroll and what they are working on. So if users notice anything suspicious, such as someone editing payroll information who they don't feel are authorised to do so, it can be reported.

Physical security measures

Secure data centers: BrightPay securely hosts its data on a remote server instead of storing it on your local desktop, ensuring optimal security measures are in place to protect it. BrightPay utilises the cloud computing service Microsoft Azure to store users' data, which is one of the leading file hosting services in the industry.

Encrypted data: As well as data being, hosted by Microsoft Azure, with BrightPay, your files will also be encrypted, meaning that the data is scrambled; making it difficult for any unauthorised people to access it.

BrightPay is integrated with 8 different accounting packages including Xero, Sage and Quickbooks, it's also integrated with HMRC, pension providers, and payment platform Modulr, meaning sensitive data can be securely transferred between the different platforms.

Legal compliance and best practices

Automated compliance: With BrightPay, you don't need to download or update to the latest version of the software, the software will always be up to date. This can give you peace of mind that you're staying compliant with regulations like GDPR or employment legislation. For example, if there is an increase to the minimum wage or a change to National Insurance rates, these will update automatically in the software.

Industry-recognised certifications: Bright's software are ISO 27001 & Cyber Essentials certified. These certifications indicate that a software provider has implemented a comprehensive set of information security controls.

At Bright, we have implemented a multi-layered approach to security. We employ a number of technical and organisational measures to help monitor and maintain the overall security posture of our infrastructure and applications, guarding them against cyber-attacks and helping to ensure the security of our clients' data.

Conclusion:

If there's one critical takeaway from this guide, it's the undeniable importance of cybersecurity in the world of payroll:

For accountants and businesses, who guard not only their own financial information but also that of their clients and employees, cybersecurity is a fundamental part of professional integrity and trust. The risks posed by cyber threats and data breaches are ever-evolving, making it essential to stay informed and vigilant.

By understanding the basics of cybersecurity, identifying potential vulnerabilities, recognising the consequences of data breaches, and implementing protective measures, you can significantly bolster your defences against cyber threats.

Leveraging cloud payroll software like BrightPay adds an extra layer of security, ensuring that sensitive payroll data remains protected.

We hope that the insights provided in this guide have equipped you with the knowledge needed to navigate the complex landscape of cybersecurity. By applying these strategies and staying proactive, you can build a safer future for yourself, your organisation, and your clients. Remember, cybersecurity is not just a technical requirement—it's a cornerstone of trust and professionalism in today's digital age.

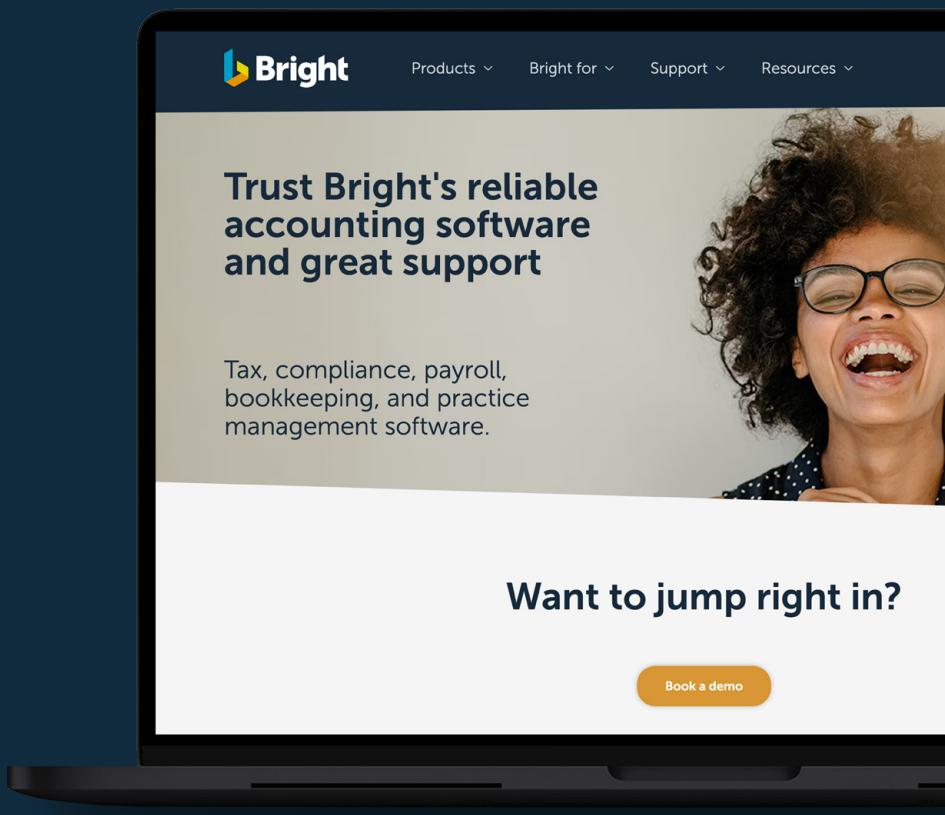
Are you ready to take the next step and try a payroll software that fortifies your defenses against data threats? You can sign up to our cloud payroll software today, using the button below. Rather try before you buy? Begin your free BrightPay trial today*, or, to see the software in action, book one of our free, online demos using the buttons below.

Sign up | **Free trial** | **Book a demo**

400,000
Businesses using Bright products

98%
Bright customer satisfaction rate

30+
Years' industry experience



Bright

Simply brilliant software

www.brightsg.com

*Our free trial is for new BrightPay customers only.