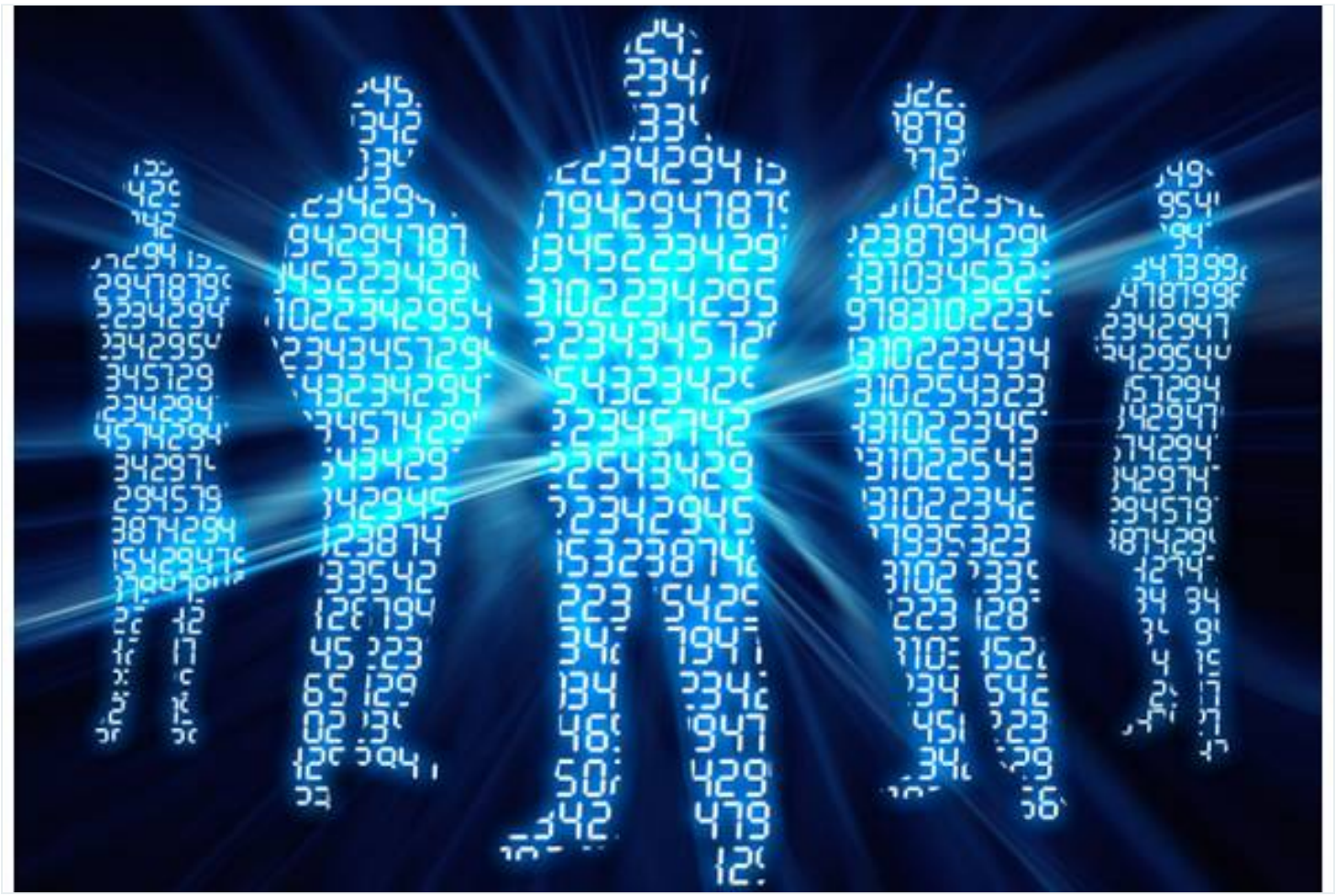
multiple threats risking the security of the payroll data you manage.

Taija Sparkman • Feb. 13, 2015



It goes without saying that employees' payroll data is sensitive and confidential information, and therefore, needs to be protected. But, it takes more than simply classifying it as "confidential" to protect it.

In today's world, there are multiple threats risking the security of the payroll data you manage. It's imperative to take the necessary steps to avoid falling victim to a cybercrime, or worse – human error. With all the news lately about data breaches, it can be easy to forget that sometimes the first line of offense is right in our own

backyards and can usually be defended against with proper training and careful

You will also want to routinely check your software for updates and/or glitches. Keeping your software up-to-date ensures that you receive the latest security patches and protection. As new viruses and threats are identified, most companies issue updates to protect against these threats. Not updating to the latest version could leave your software, and payroll data, vulnerable. In line with this, check for any suspicious or unusual behavior within the software. Does a particular process suddenly start returning an error even though the task is performed the same? This could mean there's a problem with the data entered or it could be a sign that something's wrong with the software. Perhaps an update caused an unexpected error or there's a virus. Contact the software provider to make them aware of the issue. If this is a known issue, they can develop and release a patch to fix the glitch.

Each piece of hardware that is used by your firm or your staff, including BYO devices, should have anti-virus software installed on it that is regularly maintained and used. Schedule routine virus scans and make sure that all anti-virus software is up-to-date. Make sure employees are aware of any new viruses that your systems may be prone to. Educate them on the importance of verifying payroll-related emails before they click on any links within the email or download attachments. Also, remind them to never share confidential information, such as passwords through email.

If your firm uses software that offers mobile access to payroll information, ensure that it has the same secure access that is available through their website. If the software provider uses a mobile app, test it for security features. Does it require a mobile code to access the app? Does it verify access by sending a one-time authorization code to the account holder's phone or email on file?

Lastly, you will want to meet regularly with your clients to discuss the steps and measures they are taking to ensure their payroll data remains secure. If they haven't completely outsourced payroll to your firm, or they have staff, such as HR, that

regularly accesses payroll data, make sure they have secure processes and policies in

clients' payroll data.

Payroll • Security