Why it's never too soon to review your payroll provider

South African organisations are not impervious to cyber breaches - no matter the size or industry. And not only from outside the company, but from within, too. Payroll data and records are a potential goldmine for cyber criminals because the consequences, should this information fall into the wrong hands, could be catastrophic. Sometimes with laptop theft it could have a major effect if backups are stolen, or security protocols are not in place.

Source: © Panithan Fakseemuang – 123RF.com

With October being National Cyber Security Awareness Month, companies need to think about how employees' personal information could be used to carry out identity theft. They should also consider how the organisations accounts might be hacked and emptied, says Sandra Crous, managing director of PaySpace, a leader in payroll and HR software. "Either way, incidents of this nature could quickly become public relations nightmares."

She says payroll in every organisation has the most sensitive information and making sure it does not fall in the wrong hands is critical. "Cyberattacks are growing, both in terms of frequency and sophistication. One major contributing factor is the move to remote workforces ushered in by Covid-19."

Vulnerabilities

Bad actors are cunning and smart and known to attack when experts are on leave and the business is vulnerable, such as over long weekends or public holidays. "There is always a rise in attack attempts during these times, and organisations need to be aware, particularly smaller businesses that do not have the resources for dedicated security teams and the latest technologies. Many companies don't employ two-factor authentication and rely on passwords alone. Alarmingly, many do not even use passwords," says Crous.

Moreover, she says, remote work also facilitates successful phishing attacks, not necessarily through work email alone, but through personal accounts accessed via work laptops. “People tend to feel more comfortable at home and let their guard down to a certain extent. In addition, they often use multiple personal devices, such as mobiles phones, laptops, and tablets to access the company network and applications. Without two-factor authentication, compromising these devices become child’s play for attackers.”

Organisations need to ensure they counter these threats by cyber-proofing all the apps they use, particularly when it comes to payroll, she adds.

Review and reassess

This, says Crous, is why it is critical for businesses to periodically review and reassess their payroll providers. “Make sure the provider has all the top security certifications, such as ISO 27001 and compliance with the NIST framework. While many companies use hosted applications, this is no guarantee that the provider has passed a formal security certification or sticks to best practices. If a provider does not have these certifications, look elsewhere.”

According to Crous, although many businesses relook their providers at the start of a new tax year, when it comes to cybersecurity, there’s no time like the present. “The best time to improve your security was a year ago; the second-best time is now. Don’t fall into the trap of waiting for the new tax year to review your payroll provider and security. Ransomware attacks happen every day.”

In terms of frequency, Crous says it is good to review payroll requirements annually, to ensure that the provider meets the evolving needs of the business, including security protocol, legislation changes, and business changes, such as restructuring or opening new branches abroad.

In reality, she says, sometimes businesses are resistant to change or find it uncomfortable. “This is particularly true when a business has an established relationship with a provider. However, business and technology cannot be separated from each other, and it’s foolish to endanger the business for the sake of a comfortable relationship.”

Changing a payroll provider can be a painful exercise, and one that requires time and resources. However, remaining with a provider that uses outdated technology puts the business at risk, far outweighs the effort and time to opt for a security-conscious and innovative technology provider instead.

What to look for

So, what should companies look for when choosing a new payroll and HR provider? “Firstly, ensure your provider suits your business. If you have a cloud-first strategy, never compromise on hosted solutions, and ensure you have a long-term view. Secondly, make sure the solution is scalable in both directions, as this will enable the flexibility needed to adapt to changing business needs.”

Then, Crous says to ensure your provider’s technology stack has a long-term ‘shelf-life’. “Although legacy solutions might have a mature product, they will never offer the benefits of cloud solutions, because legacy technology simply does not allow for it. Also, look for an agile implementation approach, and one with tools that can clean up your data to maximise the full benefits.”

Next, she says employee and manager self-service should be non-negotiable, enabling staff members to be more efficient and managers to have the ability to simplify and streamline what would normally be mundane and repetitive tasks.

Moreover, Crous says to ensure after-care support from the service provider, bearing in mind that support should have the required legislative, payroll and HR experience to support your product. “Look out for costing models that are truly consumption-based, not feature-based.”

In closing, Crous says to carry out a thorough investigation of multiple service providers before choosing one. “Consult reference sites to ensure the size and complexity of your business can be adequately catered for. Ease-of-use and maintenance should never be underestimated. Don’t invest in software with expensive maintenance costs where changes and updates depend on the service provider. Make sure the roll-out and success of the product are in your hands.”