access
freedom to do more

EBOOK

The Cybersecurity Risk for Payroll

How to protect your organisation's payroll from the growing risk of cyberattack

Is your payroll data safe from the growing threat of cybercrime?

Cyberattacks have steadily increased in Australia since the start of the COVID-19 pandemic, with organisations firmly in the crosshairs.

In the 2020-2021 financial year, over 67,500 cybercrime reports were made to the federal Government's cybercrime protection agency, the Australian Cyber Security Centre (ACSC). The figure represents a 13 percent increase from the previous year, amounting to $33 billion in self-reported losses.[1]

The tactics of cybercriminals are ever evolving, with many Australian organisations–and their payroll departments–posing as lucrative targets. The sensitive personal information which payroll holds on employees, like their bank account details, home addresses, and wage information, are highly sought after by cybercriminals and often later used for the purposes of re-routing wages or even identity theft.

When an organisations' employee data is compromised by cybercriminals, the payroll fraud that follows often results in millions in stolen wages.

Just this year, alleged cybercriminals in Adelaide and Sydney were accused of stealing more than $11 million by hacking into organisations and modifying payroll, superannuation, and credit card details.[2]

So what can your payroll team do—and your organisation more broadly—to help safeguard your critical payroll data from the growing risk of cybercrime and data breaches?

In this guide, we outline the cybersecurity risk facing Australian organisations and the costly implications of suffering a cyberattack and or data breach. We also highlight five specific types of cybersecurity threats facing organisations and their payroll departments. And we provide five measures payroll teams and their organisations can implement to help boost cybersecurity.

[1] ACSC Annual Cyber Threat Report 2020-21

[2] https://www.austpayroll.com.au/alleged-cyber-criminals-in-adelaide-sydney-charged-over-11-million-identity-theft/

The risk of cybercrime and data breaches for Australian organisations

Since the start of the COVID-19 pandemic, Australian organisations have faced a complex and evolving cyber threat environment.

Since the start of the COVID-19 pandemic, Australian organisations have faced a complex and evolving cyber threat environment.

With so many employees working from home during this time, we saw corporate computer networks expand into the homes of employees. The shift to this new working arrangement was rapid, and as such, many organisations deployed remote networking solutions quickly, often to the detriment of their cybersecurity.

Cybercriminals repeatedly took advantage of the heightened vulnerability of Australian organisations not only to steal their sensitive employee data, but also that of their customers, and to conduct espionage, steal money, and disrupt services. In 2020, 89% of Australian cybersecurity professionals said attacks increased due to employees working remotely.[3]

Data breaches and their cost to Australian organisations

A data breach that exposes the personal information of employees can create a nightmare scenario for an organisation and its payroll team.

In the 2020-2021 financial year, there were 985 data breaches suffered by Australian organisations, which led to the exposure of personal information of either employees or customers. The average cost of a data breach in Australia is $3.35 million per breach, an increase of 9.8% year-on-year. [4]This, in addition to the significant reputational damage which an organisation can suffer.

Are Australian organisations unprepared for the risk of cybercrime?

What's even more alarming is that according to Varonis, a leading Australian cybersecurity firm, organisations take an average of 233 days to detect and contain a data breach. Despite this, 82% of organisations rate their ability to protect themselves from a cyberattack as good or very good.[5]

The rise of data breaches since the start of the COVID-19 pandemic, coupled with the slow response times of Australian organisations to cyberattacks, point to a serious overconfidence in their ability to protect themselves against cybercrime.

[3] Australian Security Insights Report 2021, VMware

[4] https://www.ibm.com/blogs/ibm-anz/the-rising-cost-of-a-data-breach-in-2020/ 2021 Australian Cybersecurity Risk Report, Varonis

What are the key cybersecurity threats facing payroll teams?

Cybercriminals are continually evolving their tactics to penetrate the security apparatuses of Australian organisations, and one of their key motivations is to gain access to or steal employee data.

According to a 2021 survey conducted by Varonis, Australian organisations believe the personal data of employees is just as much of a target as business-related data. 61 percent believe the most likely target for a cyberattack is sensitive personal data, ahead of both the organisation's financial details (58 percent) and customer financial details (55%).[6] But as you will see below, it's not only malicious outside actors who pose a threat to the data security of Australian organisations.

Let's look at the main tactics used by cybercriminals to gain access to the employee data of Australian organisations, and how human error also poses a significant risk.

1 Ransomware

The Australian Cyber Security Centre reports that ransomware "poses one of the most significant threats to Australian organisations," and in the 2020-21 financial year, this variety of cyberattack increased 15 percent.[7]

In ransomware attacks, cybercriminals infiltrate an organisation's computer systems and infect it with ransomware – a form of malicious software that renders devices or files inaccessible. Cybercriminals often steal and encrypt data, or damage internal networks, and demand money to undo it.

In recent years, several high-profile Australian organisations have fallen victim to ransomware attacks, with catastrophic results. In 2020, 26 percent of all data breaches in Australia were caused by ransomware.[8]

[6] 2021 Australian Cybersecurity Risk Report, Varonis

[7] ACSC Annual Cyber Threat Report 2020-21

[8] Australian Security Insights Report 2021, VMware

2 Phishing

Phishing is a tactic whereby cybercriminals attempt to trick the recipient of an email (or in some cases, a text message) to give out personal information. Often, phishing emails pretend to be from a large organisation that the recipient may trust and contain a link to a fake website where they are encouraged to enter confidential details.

There are also phishing scams that target payroll professionals specifically. These fake emails typically request a change in bank account details and appear to use an employee's correct sender name and email signature.

3 Hacking

Hacking is now a well-known tactic of cybercriminals which involves the unauthorised penetration of a system or network, often to exploit a system's data. The methods by which cybercriminals can bypass an organisation's IT security system varies. It could be by using software code designed to penetrate IT security systems, cracking a password, or exploiting existing security vulnerabilities.

4 Malicious insiders

Malicious insiders can be either present or former employees, or perhaps contractors who have legitimate access to your payroll systems and data, but use that access to destroy or steal data. According to Varonis, 37% of Australian organisations view insider threats as their biggest cybersecurity concern.[9] Malicious insiders don't include well-meaning staff who accidentally put your cybersecurity at risk or spill data.

[9] 2021 Australian Cybersecurity Risk Report, Varonis

5 Human error

In many cases, personal employee information can be released to unauthorised people by human error. For example, an email with personal information can be sent to the wrong person, or a device containing personal information is lost.

According to Varonis, 40% of Australian organisations view human error as their biggest cybersecurity concern.[10] And the concern is warranted. In the 2020-21 financial year, human error accounted for 34% of Australian data breaches reported to the Office of the Australian Information Commissioner.[11]

[10] 2021 Australian Cybersecurity Risk Report, Varonis

[11] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021

How can you safeguard your payroll data?

The cybersecurity risk that Australian organisations face has never been greater.

In the 2020-21 financial year, the Australian Cyber Security Centre received an average of 184 reports of cybercrime every day.[12] And according to Varonis, almost two thirds (63%) of Australian organisations believe it's very likely or likely that they will be a target of a cyberattack in the next 12 months.[13]

It's therefore critical that your payroll team—and your organisation broadly—does all it can to make cybersecurity a priority. So what are the key preventative measures your payroll team can take to protect your data and systems?

1 Educate employees about cybersecurity

Research by Australian cybersecurity firm Security In Depth reveals that 38 percent of Australian organisations have never provided cybersecurity training to their staff, and that 55 percent have no cyber governance framework in place.[14]

While such training measures may be the imperative of your organisation' leaders, HR and payroll teams are uniquely positioned to lobby for and establish such measures, to ensure there's a culture of vigilance within the organisation. This could mean creating policies to help employees understand what is acceptable when they use or share data, computers and devices, emails, and internet sites.

It could also entail educating staff about the cunning methods hackers employ, so that they will know what to look for to prevent cyberattacks. For instance, you could conduct simulated phishing campaigns to encourage employees to report suspicious emails to the HR team.

[12] ACSC Annual Cyber Threat Report 2020-21

[13] 2021 Australian Cybersecurity Risk Report, Varonis

[14] State of Cybersecurity 2019 Annual Report, Security in Depth

2 Control access to your payroll systems

To ensure your payroll systems are secure from unauthorised access, there's no understating the importance of regularly updating your passwords—and ensuring they are strong. While many organisations invest heavily in cybersecurity, passwords are often overlooked as a key line of defence. According to IBM, 82% of all data breaches result from weak or compromised passwords.

In addition to a strong password, it's also wise to use multi-factor authentication if offered by your payroll software. This form of security not only requires a username and password to log in, but also a code that's sent to your phone. This means that without your phone, your account can't be accessed by hackers.

It's also important to monitor the use of your payroll system and keep track of any out of hours or unusual access. And if you can, it's a good idea to limit access to your payroll system. Many leading payroll solutions offer robust security options that allow you to control access, including specifying add, edit and delete privileges for specific staff members.

3 Perform regular data backups

Varonis research reveals that one in five Australian organisations are less than confident about the location of their most sensitive data, including employee personal information.[15] If your payroll data is accidentally deleted, or rendered inaccessible by malicious outside actors, it could spell disaster for your organisation if it hasn't been performing regular data backups.

Notwithstanding the potential fines and reputational damage that comes with exposing or losing access to employee personal information, the costs and downtime of recovering that data–and getting your payroll operation up and running again–could be catastrophic to your organisation. Failing to pay your employees on time could be just one of the problems you face in such a scenario.

It's therefore critical that your organisation has a backup and disaster recovery strategy in place. This should include saving backups to an offsite facility, rather than in-house, to ensure they won't be impacted by a potential cyberattack.

[15] 2021 Australian Cybersecurity Risk Report, Varonis

4 Create a cyber incident response plan

If your employee data is exposed and or stolen in a cyberattack or data breach, does your organisation have a place in place to mitigate the effects and help speed its recovery? Research by Security In Depth reveals that only 37 percent of organisations have developed and implemented a cyber incident response plan, and only 17 percent have tested it.[16]

The Office of the Australian Information Commissioner (OAIC) provides a detailed, step-by-step guide to prepare for and respond to data breaches. And if your organisation is covered by the Privacy Act 1988, it's critical to understand its obligation to notify individuals and the OAIC in the event of a data breach which discloses personal information. Please visit the OAIC website for more information on what the National Data Breach Scheme requires in such scenarios.

5 Use a trusted payroll system

It's essential that you choose a payroll software provider with a proven track-record of offering secure solutions, and one that takes a proactive approach to ensuring the cybersecurity of its clients. Such vendors offer payroll software that is ISO certified, regularly subjected to penetration testing, and backed by an experienced team of experts who understand the importance of cybersecurity.

[16] State of Cybersecurity 2019 Annual Report, Security in Depth

Ensure a secure, efficient payroll operation with The Access Group

For over 35 years, Access payroll solutions have been trusted by Australian organisations not only to streamline their payroll, but also ensure the security of their employee data. Discover how you can ensure the cybersecurity of your payroll operation with our proven and tested payroll solutions that are designed for Australian organisations.

Discover more

About The Access Group

The Access Group is one of the leading providers of business management software to UK, Ireland and Asia Pacific mid-market organisations. It helps more than 55,000 customers across commercial, public sector and not-for-profit sectors become more productive and efficient. Its innovative Access Workspace cloud solutions transform the way business software is used, giving every employee the freedom to do more. Founded in 1991, The Access Group employs more than 3,850 staff.

For more info, visit: **www.theaccessgroup.com/en-au**
or contact us at **1300 729 229**

access
freedom to do more