Case study – Cloud Security

When the cloud-based service you rely on has a breach

"Breach uncovered – potentially significant number of job applicant personal details inappropriately disclosed" …. blasted headlines in the major online publications. A number of organisations, both private and public relied on PeoplePages as an extension to their HR recruitment processes. With awareness of the breach increasing, what questions would get raised by senior management and what impacts would it have on us?

Synopsis

The Department of Innovation leverages the use of PeoplePages – a Software as a Service cloud-based HR platform to improve its recruitment processes. Its usage becomes more pervasive over time including applicant onboarding and payroll setup. PeoplePages experiences a breach where information from the department has been disclosed in an unauthorised way. When trying to determine what went wrong, senior management try and review if adequate risk management was conducted at initiation and throughout the usage of the service. This case study is modelled on a real breach that occurred with PageUp People in June 2018.

Background

On 8 June 2018 Remy Novak – Chief Risk Officer of the Department of Innovation –walked through the front door when she was confronted with a sea of panic.

“Remy! Did you hear about the breach? What are we going to tell Terence?” asked John Wigley – Chief of Operations.

Terence Klein, Secretary and sceptic of the adoption of cloud services within the department will have a field day with this one. Remy knew that they had leapt straight into using PeoplePages, based on pressure they had received from their HR function and the negative impact the legacy system had been causing them. But she wondered how diligent they had been through the initial risk assessment and subsequent governance of the service [1].

Even now, she was not sure if she could answer how the Department was affected and what information was potentially compromised.

Up, up and away

“No, I’m telling you, our existing system has so many issues that it’s negatively impacting our recruitment and that is having a flow on effect to the department. Considering we’re the Department of Innovation, we sure aren’t very innovative, are we?!” bellowed Emma Lawrence, Head of People and Culture. “We’ve already done a market scan and PeoplePages is the most suitable solution for us. Besides, it’s in ‘the cloud’, it’s not like we even need our own IT people to do anything. Procurement said it’s fine [2]. I don’t see what the big fuss is about.” She added, her patience completely depleted.

“Well, I’m not really comfortable going ahead unless we’ve done some due diligence and appropriate risk assessment. We need to at least understand what information we’re going to transfer and receive, what value this information is and what security measures this service has in place [3”]. Remy replied – as level-headed as any diligent risk professional could be.

“Look Remy, I know we’ve all got a job to do here, but honestly, all we’re doing is switching from the old broken system we have, where applicants apply for a job and using this new platform instead. It’s easier, it’s cost effective and they even do the preliminary screening for us. They give us the details of the short list of applicants so we can get on with recruiting instead of wasting our time with system issues. Terence already gave it the go ahead. I mean, it’s not like we’re sharing classified blue prints with them or something.” It was almost as if Emma was talking over her shoulder, half physically departed from the conversation already.

Remy thought that more should be done. “Perhaps we should understand what controls we expect there to be in place. Aren’t they still a third party after all and subject to the same third party risk management approach?” [4] she pondered.

While she appreciated that the information may just be job applicant information, didn’t the department have some responsibility for that information once they received it? [5] She had more questions than time to deal with, and given the Secretary had already decided to go ahead, she decided to prioritise her focus on more pressing “watermelon risks” (risks that were being reported as green but clearly were in the red).

It was January 2016, and it was way too early in the year to start a new confrontation unnecessarily.

Clouds do move sideways

“Since we signed up PeoplePages, we’ve streamlined our recruitment process to get a new hire in from 3 months to 6 weeks, Terence. We’ve been able to meet 95% of outstanding recruitment requests, that’s a major improvement on our prior 50% rate. And now with the further integration, PeoplePages are suggesting where they will also perform security clearance checks, onboarding, and payroll setup, we are going to see further improvement. All we need to do is accept the extension of these services and uplift the current license”. Emma beamed with the amazing results she and the team had achieved. “It’s been one year, and the results are outstanding. This should be a no brainer.”

“You know I’m not very comfortable with these cloud services, but your results are impressive. I agree, let’s go ahead if it’s going to continue to lead to further improvement” Terence endorsed.

“Hang on, if we’re looking to integrate systems and share information at a system level, then we definitely need to do a more diligent risk assessment compared to when we first signed up [6]. I wouldn’t be comfortable with us proceeding, and I’m sure I can safely speak on behalf of Barry (the CIO) that he wouldn’t be either, until we have a really thorough understanding of what this integration is going to mean. We have obligations under the Victorian Protective Data Security Standards to ensure that relevant controls exist at PeoplePages when we share information with them.” Remy stated, not backing down this time.

Two weeks passed and Remy’s team had come back with the results of the more detailed assessment. “We’ve assessed the risk as high. Because it’s a Software as a Service, we don’t have any ability to directly manage the controls of the service, we can only largely rely on contractual clauses. You are aware, that even if we are just talking about personal data relating to job applicants - both prospective and hired - once we receive it from PeoplePages, we are now responsible for that data and need to protect it to the same level that we treat our own personal data. As a result, I’m suggesting that we don’t proceed until we have a more thorough review of PeoplePages’ controls and we are comfortable with how they protect information and more importantly, what happens if there’s an incident. We aren’t against the usage of Software as a Service cloud platforms by any means, but we need to understand that the way manage controls is different and we need to take that into consideration.” Remy relayed, pointing out the overall risk the department would be subject to.

“Well, as the business owner I’m happy to sign off and accept the risk. I appreciate your input Remy, but Terence has already given us approval to proceed” [7]. Emma, again, had already moved on from the point.

Not all clouds have a silver lining

On 8 June 2018, the leadership team were in a briefing session on the PeoplePages breach.

“Based on the risk assessment we performed prior to system integration, we were aware of the information that we were sharing and would receive. As the business had accepted the risk, we agreed that we would continue to periodically monitor and assess the risk, but we haven’t done this prior to the breach. We have little knowledge of how many of the exposed records relate to us and what this means for us. When the system was shut down while they investigated the breach, we had to resort to prior manual processes. While we responded to the incident once we had heard about it in the media, our incident response processes were not up to scratch to identify and deal with the incident earlier on when it was first detected by PeoplePages [8].

While we appreciate the frequent updates we have received, PeoplePages has not been able to fully determine the impact yet. At this stage, we’re at an impasse. For all we know, this could be catastrophic

and we could be facing a situation where we have unwillingly disclosed a number of personal records that we were responsible for protecting. Other departments such as the Department of Safety who did go through appreciate risk assessment and put specific controls in place, have been able to make more effective recovery efforts and as a result have been less impacted[9].

Remy was doing her best to stay level-headed and not dive into "I told you so" mode. After all, Emma's team had been pulling long days as they resorted back to manual processes that – as everyone recalled – already had issues to try and alleviate the impact of the system outage. If not for anything else, Remy knew that from this point on, the department would be far more diligent for the next cloud service requirement.

Conclusion

A cloud service, despite its certifications and assurances, should be subject to an appropriate third-party risk assessment, prior to engaging the service and on an ongoing basis.

There needs to be an understanding of the type of information that is shared and received, by undertaking a Business Impact Level assessment and determining the value of this information to determine how the information needs to be managed.

Ongoing governance of the service is key, not just to validate the service is being used as it was initially designed, but that the controls stated by the service provider are valid. Incidents may still occur, appropriate incident response plans linked in with the service provider and appropriate business continuity measures should be in place. Even if the business chooses the accept the risk, ongoing monitoring and re-assessment of the risk is critical especially if the risk is potentially high.

The facts

While the characters and events in this case study are fictional, it was based on the actual PageUp breach that occurred in June 2018. While PageUp indicated that the breach did not result in information being exfiltrated, the information was accessed and viewed.

Find more information about the breach here:

https://www.cyber.gov.au/news/pageup-data-incident

Impacts of poor third party security

What was affected	Impact
Personal / Injury	Personal information of 45,000 job applicants (including those from 14 agencies) could lead to identity fraud.
Financial	People hours required to respond to the incident on average, 3 full time staff for one week per affected agency. This in turn leads to, business opportunity cost and additional labour cost.
Service delivery	On average, 3 full time staff for one month per affected agency are

	required to revert to and manage the manual process therefore a business disruption, opportunity cost and additional labour cost.

Alignment to risk

'**The risk of** ….event…. **caused by** ….how…. **resulting in** ….impact(s)…'.

This case study may manifest itself as the following risk statements in a risk register:

1. The risk of	2. Caused by	3. Resulting in
Unauthorised access/disclosure of personal information.	Cybercriminal(s) targeting vulnerabilities in the application	Impact to individuals whose personal information was affected; service delivery; and/or financial impact.
Intentional system disruption.	Malicious external actors.	Financial impact and business disruption.

Key flags and control considerations

Flag	Issue	Control considerations	Element reference
1	Thoroughness of initial assessment in relation to cloud services.	A consistent method for identifying and assessing the risks of cloud services (Software, Platform and Infrastructure) is important to assist the business in determining the risks of adopting cloud services. *Standard 3 – Information Security Risk Management: E3.010, E3.020*	*E3.010* - The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: • Risk identification; • Risk analysis; • Risk evaluation; and • Risk treatment. *E3.020* - The organisation records the results of information security risk assessments and treatment plans in its risk register.

Flag	Issue	Control considerations	Element reference
2	Alignment of procurement and third party risk management practices.	With appropriate governance models, procurement can assist with identifying any risks of new cloud services and implementing any mitigations before procuring the service. Examples include adding/appending relevant clauses in the contract for annual assurance/right to audit. *Standard 8 – Third Party Arrangements: E8.020, E8.030, E8.040*	*E8.020* - The organisation includes requirements from all security areas in third party arrangements (e.g. contracts, MOUs and information sharing agreements) in accordance with the security value of the public sector information. E8.030 - The organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement. *E8.040* - The organisation identifies and assigns information security roles and responsibilities in third party arrangements (e.g. contracts, MOUs and information sharing agreements).
3	Understanding the information assets being shared and the business context.	In order to appropriately assess the risk and determine what obligations may need to be considered, understanding what information will be shared and how it is used is critical. *Standard 2 – Information Security Value: E2.020, E2.040, E2.070*	*E2.020* - The organisation identifies, documents and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders. *E2.040* - The organisation identifies and documents the security attributes (confidentiality, integrity and availability business impact levels) of its information assets in its information asset register. *E2.070* - The organisation continually reviews the security value of public sector information across the information lifecycle.

Flag	Issue	Control considerations	Element reference
4	Consistent application of a third party risk management approach.	Cloud services are like any other third party and should be subject to the same third party risk management and governance controls. *Standard 8 – Third Party Arrangements: E8.030*	*E8.030* - The organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement.
5	Information ownership and responsibilities.	In relation to personal information, if an organisation receives that information (even via a service), then they become responsible for the protection of that information. *Standard 2 – Information Security Value: E2.080*	*E2.080* - The organisation manages externally generated information in accordance with the originator's instructions.
6	Cloud service usage scope may change quite dynamically and often without any form of reassessment.	Establishing triggers is important to reassess the risk of how a cloud service is being used. This is especially the case when additional functionality is being introduced and/or additional forms of information may be shared. In addition to undertaking reviews based on certain events being triggered, undertaking periodic revalidation of the third party's security requirements where identified gaps are committed to be addressed by the third party will ensure continuous improvement. *Standard 8 – Third Party Arrangements: E8.060*	*E8.060* - The organisation monitors, reviews, validates and updates the information security requirements of third party arrangements and activities.

Flag	Issue	Control considerations	Element reference
7	Acceptance of risk at a business level may lead to situations where the risk is not appropriately monitored and reassessed on an ongoing basis.	With appropriate information, business acceptance of a risk is an acceptable position. It is recommended that even when risks are accepted, if they are sufficiently high, they should be monitored on an ongoing basis and where need be, reassessed. *Standard 3 – Information Security Risk Management: E3.050*	*E3.050* - The organisation governs, monitors, reviews and reports on information security risk (e.g. operational, tactical and strategic through a risk committee (or equivalent, e.g. audit, finance, board, corporate governance)).
8	Existing incident management processes may not necessarily provide coverage over incidents arising from cloud environments.	When reviewing incident management processes, it is important to understand the roles and responsibilities should an incident arise with the cloud service provider including how it engages with the service provider to receive notifications in a timely manner and how the organisation can manage these incidents in the most effective manner. *Standard 6 – Information Security Incident Management: E6.020, E6.030*	*E6.020* – The organisation articulates roles and responsibilities for information security incident management. *E6.030* - The organisation's information security incident management processes and plan(s) contain the five phases of: • Plan and prepare; • Detect and report; • Assess and decide; • Respond (contain, eradicate, recover, notify); and • Lessons learnt.

Flag	Issue	Control considerations	Element reference
9	Having identified risks aligned to appropriate business continuity management in order to recover from incidents.	The effective management of risk may require appropriate identification of business continuity management policies and plans to allow for suitable recovery from the incident whilst keeping business operating with minimal impact. *Standard 7 – Information Security Aspects of Business Continuity Management and Disaster Recovery: E7.010, E7.020, E7.030*	*E7.010* – The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas. *E7.020* – The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans. *E7.030* - The organisation regularly tests (at least annually) its business continuity and disaster recovery plan(s).

Suggested next steps

Implementation or uplift of controls covering:

- **Risk management** – ensuring the risks associated with cloud providers are identified and managed for the life of the arrangement;
- **Third party arrangements** – ensuring the same methodology is applied to cloud providers as any other service;
- **Information management** – knowing where the organisation's information is and who has access; and
- **Incident management** – ensuring appropriate incident detection and response processes and plans are in place regardless of where the organisation's information is.

More information

Contact OVIC at security@ovic.vic.gov.au if you would like to discuss this case study further.

Further Information

Contact Us

t: 1300 00 6842
e: security@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer