

Case study – Personnel Security

An inside threat: The Rotten Apple



It was another blow to the reputation of a highly visible government department. While messages on Twitter focused on building trust, the media gained more ammunition to highlight corruption and poor governance in a sector that was already trying to do the best with what they have. Yet, that was the harsh reality posed by Frank Tephlon, Project Manager for the Department of Cultivation as he responded to the Audit and Risk Committee about personnel issues that led to unauthorised and unethical behavior from one of his team.

Synopsis

Government organisations had been singled out in the news recently after a string of corruptions across agencies had been uncovered. The public expected government entities to deliver value in a way that was consistent with and reflected public values. Due to the spate of corruption cases, public trust in government entities had diminished. Government organisations were seeking to demonstrate more transparent practices to citizens to try to address this concern.

The Department of Cultivation found themselves in hot water, after it emerged that an employee had handled/used sensitive information unethically, possibly over an extended period of time. This came as a surprise to senior management who tried to determine the ramifications of this incident, and what measures were in place to address personnel security.

Background

A significant project involving the payroll system was underway in the Department of Cultivation. Senior management were placing intense pressure on the team, expecting the project to be delivered in four weeks.

The project team thought this timeframe was unreasonable as a similar project had previously taken eight weeks. The team was assured by the project manager, Frank Tephlon, “don’t worry, I’ve been given the go ahead to hire extra people resources to get us across the line because of how time critical this is.”

Given the team pressures, and at Frank’s behest, human capital partner Sally Leftcross opted to use a recruitment agency called HireHelp to assist in getting someone on board quickly. HireHelp were eager to assist and came back with fast results – “Hi Sally, we’ve got just the right person to come in and assist with your project. He has experience working in government agencies and a solid resume working in a range of different roles. We’ll send John’s details through to you.”

Sally accepted John’s application, assuming that HireHelp had conducted their due diligence and performed the appropriate background and reference checks ¹; as they were a top recruiting agency.

A new beginning

John Lightfingers was brought into the Department quickly. He was relieved that he got the role despite recently being fired from his previous job, after his former boss cited ‘unethical behaviour’ as the primary reason for letting him go.

John was surprised at how quickly he went through the recruitment process and figured that his previous experience in government agencies must have been highly regarded.

After becoming familiar with some of the key systems, John noticed that his role in the Department granted him an abnormally high level of access to Corporate Systems, including access records containing privileged information ².


This information contained not only intellectual property pertaining to the project, but also access to personal information of the Department’s many stakeholders.

An opportunity you can’t refuse


After settling into the role, and getting comfortable with the departmental systems and processes, John saw an opportunity to profit from his access to the organisation’s information. In previous roles, John had some nefarious side dealings with shady third parties where he had fed public sector information for favours and kickbacks.

Unsuspecting of John’s intentions, Project Manager Frank hurried out of the office one evening, passing John on his way out – “staying back late John? Good to see you putting in the extra effort- there might be something longer term for you since I’m quite impressed on how you are tackling the project”.

After waiting for his other colleagues to leave, John opened the payroll system and started looking through one of the databases that contained personal information. He noted several hundred rows of valuable information and thought how easy it would be to get away with manipulating this information. After all, there was minimal system logging and little oversight of his account. He thought he may as well make some


money off his access and started planning to exfiltrate the data when he had more time 3.

The heist

After spending a few more evenings familiarising himself with the system, John figured it was the right time to strike. As usual, Frank and his other colleagues left around the usual time and John opened the payroll system once again. He prepared the information by exporting it first into an excel spreadsheet which he then extracted to a USB drive 4.

John knew he could profit from the information he had managed to copy from the Departmental systems. Suddenly he received a tap on the shoulder from Frank. “Doing some spreadsheet manipulations for the project I hope?” said Frank.

Frank had returned to the office with his colleague Mark after leaving his keys on his office desk. Startled, John managed to close the spreadsheet and quickly make up a story which confirmed Frank’s suggestion. Frank was satisfied with John’s explanation – “Only kidding John, have a good evening - you should go home and get some rest!”


Mark had also been working on the payroll project and was less convinced as he knew that system wasn’t part of what they were working on. However, he didn’t feel it was his responsibility to say something as it was above his pay grade and it was ultimately Frank’s job to manage John 5.

Caught in the act

It had been two weeks since John extracted the information from the departmental system, and he had managed to go undetected in his malicious after-hours activities.

John thought his colleagues were ignorant to his behaviour, but Tracy had also been working back late after hours. She had come across some suspicious content on John’s screen one evening while John was away from his desk. She was unable to capture any evidence at the time but decided she would say something to alert management.

While Tracy wasn’t a part of the payroll project team, she pulled Frank aside to have a quiet conversation with him, “I saw John looking through personal information and he had his personal emails open messaging someone.”

Frank launched an initial internal enquiry into John Lightfingers access of records. The enquiry identified some evidence that John had been conducting unauthorised searches of stakeholder records but could only establish a loose correlation between his system activity and Tracy’s initial report 6.

Thrown right back at you

Despite the way Frank felt, he had enough to question John. However, when confronted, John denied the reports and dismissed the little evidence the team had managed to gather.

When Frank pushed him for more information, John started to fire back, accusing Frank of tarnishing his good name and discriminating against him. John argued that the evidence was weak and didn’t prove any wrongdoing. Frank begrudgingly accepted John’s claims, and the investigation moved sideways for the time being. John’s behaviour was not sanctioned and no disciplinary action was taken.

John resumed his work on the project. There was a rift between both parties and an additional concern


that the project would not be completed to the required standard. Frank decided that he would keep John on the project until completion, and eventually move him off the team. Frank believed it was too hard to performance manage him and hoped someone else could deal with him.

A swift exit

Frustrated with recent developments and the probes into his wrongdoings, John started to look for work in another government agency.


He knew that the Department of Cultivation had a follow up meeting scheduled to go over the purported incident. As the payroll project was coming to a close, he saw this as a prime opportunity to make a swift exit from the agency and avoid further reprimand or potential prosecution.

He knew he would need to come up with a cover story in case anybody asked about his brief tenure with the Department of Cultivation but didn't think this would be too difficult given his understanding and experience of working in government.

After looking around and networking, an associate directed him to a similar role within the Department of Youth Health. John applied for the role and was snapped up 7. Upon resigning, he told his project colleagues that "Department of Youth Health offers better opportunities and will mean that I can move onto bigger and better things."

Upon John Lightfinger's departure, the internal investigation looking into the incident ceased without any further follow up. The Department of Cultivation was not going to waste time and effort in investigating the incident.

Despite this, local management reported their initial findings to the Audit and Risk Committee who were not fully satisfied with how management handled the situation. They subsequently requested Frank to attend the next committee meeting to discuss the matter further.

In the meantime, John took up his new role of system manager at the Department of Youth Health. He decided to check if he was still able to log into his old work emails using his old remote access token which Department of Cultivation failed to take off him after he left 8. He found he still had access! 'Brilliant!' he thought – John was pleased that not only had they forgotten to take the token off him, but it looks like they failed to disable his access as well. This gave John plenty more time to see what other info he could get his hands on.

Conclusion

Organisations should ensure that the people who have access to government assets are eligible and suitable. Organisations should define and implement strong personnel screening processes and provide training for all persons on how to use and manage organisational assets – including public sector information and systems.

Organisations should carefully manage all personnel (full time, contractors, consultants, volunteers, etc.) across all stages of the personnel lifecycle. Lifecycle phases include:

- pre-engagement (before they commence work with the organisation);
- engagement (monitoring them whilst they are actively engaged or at the point, they are re-engaged); and

- separation (when they leave either temporarily or permanently).

Organisations should actively review, validate, and update their personnel security policies and procedures, and embed these security requirements into HR and local work management practices.

The facts

This case study was inspired by real events in Victorian public sector organisations where personnel security measures weren't observed or were assumed to be operating effectively.

In one instance a corrupt employee leveraged their position within an agency, enabling criminal activity.

More information about this event and similar stories relating to personnel security can be found here:

<https://www.theage.com.au/national/victoria/brothel-owner-bribe-claims-against-planning-officer-20120929-26shs.html>

<https://www.theage.com.au/politics/victoria/he-was-doing-a-great-job-darebin-s-16m-council-corruption-scam-20190930-p52w95.html>

<https://www.heraldsun.com.au/news/law-order/victoria-polices-taskforce-keel-shuts-down-after-investigating-serious-security-breaches/news-story/57e5d11d1a5812597755a502c082de29>

Impacts of poor personnel security

What was affected	Impact
Personal / Injury	The confidentiality of information is compromised especially when coupled with lackluster ICT access controls potentially adversely impacting the individuals whose personal information was disclosed.
Service delivery	The information was altered in a malicious way, compromising its integrity therefore reducing its quality or rendering it unusable impacting effective service delivery.
Reputation	If enabling criminal activity is associated with a Victorian public sector organisation, this is not only embarrassing for the organisation, but also reduces public trust from the local community. This creates a new barrier for government organisations when engaging with the community.
Legal / Compliance	The organisation chose to undertake a misconduct investigation that was managed internally and impacted internal resources.

Alignment to risk

‘The risk ofevent.... caused byhow.... resulting inimpact(s)...’.

This case study may manifest itself as the following risk statements in an organisation’s risk register:

1. The risk of	2. Caused by	3. Resulting in
Unauthorised access/disclosure of personal information or intellectual property	Privileged employees abusing their access	Impact to individuals whose personal information was affected; reputation damage and/or financial impact
Unauthorised modification of personal information or intellectual property	Privileged employees abusing their access	Degradation of quality and service delivery
Intentional system disruption (sabotage)	Malicious / disgruntled employees	Financial impact and business disruption

Key flags and control considerations

Flag	Issue	Control considerations	Element reference
1	Undertaking pre-employment screening and security vetting.	The hiring manager should follow appropriate pre-employment screening and security vetting processes to highlight any issues early on in the process and manage any risks identified. <i>Standard 10 – Personnel Security: E10.030</i>	<i>E10.030</i> - The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.

Flag	Issue	Control considerations	Element reference
2	Roles and permissions commensurate to the level of access required for a user.	<p>A user's role and permissions should be limited to the amount of access required to perform their functions and limit unnecessary exposure of information. These permissions should be reviewed on a regular basis.</p> <p><i>Standard 4 – Information Access: E4.010, E4.020, E4.040, E4.070</i></p>	<p><i>E4.010</i> - The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know.</p> <p><i>E4.020</i> - The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information.</p> <p><i>E4.040</i> - The organisation implements logical access controls (e.g. network account, password, two-factor authentication) based on the principles of least-privilege and need-to-know.</p> <p><i>E4.070</i> - The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.</p>
3	Monitoring user behaviour and identifying events of interest.	<p>Monitoring for user behaviour, especially events that are deemed as suspicious/abnormal are crucial to detecting and maximising preventing a breach from occurring.</p> <p><i>Standard 11 – Information Communications Technology (ICT) Security: E11.110</i></p>	<p><i>E11.110</i> - The organisation logs system events and actively monitors these to detect potential security issues (e.g. intrusion detection/prevention systems (IDS/IPS)).</p>

Flag	Issue	Control considerations	Element reference
4	Managing removable media.	<p>Governing acceptable use of removable media with people, process and technology controls is important to minimise the likelihood of a security incident involving the introduction of threats via removable media and/or limiting opportunities for data exfiltration.</p> <p><i>Standard 11 – Information Communications Technology (ICT) Security: E11.080</i></p>	<p><i>E11.080</i> - The organisation manages security measures (e.g. classification, labelling, usage, sanitisation, destruction, disposal) for media.</p>
5	Security is everyone's responsibility.	<p>The organisation conducts regular personnel checks e.g. police checks, probity checks on staff in identified roles.</p> <p><i>Standard 10 – Personnel Security: E10.040</i></p> <p>All staff understand their information security obligations including their role in reporting suspicious behaviour and they feel comfortable to notify someone if they feel inappropriate activity may be occurring.</p> <p><i>Standard 5 – Information Security Obligations: E5.030</i></p>	<p><i>E10.040</i> - The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.</p> <p><i>E5.030</i> - The organisation delivers information security training and awareness to all persons with access to public sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.</p>

Flag	Issue	Control considerations	Element reference
6	Undertaking appropriate logging and monitoring for forensic evidence.	<p>Should the need arise during and/or post incident to understand how an event occurred so it can be presented as evidence, appropriate capabilities should exist to monitor, log and record events in a well-structured and forensically sound manner.</p> <p>The organisation proposes an improvement to the incident management control including performing alerting to key stakeholders as soon as an incident is detected. It also includes identifying an increased frequency for monitoring key risks.</p> <p><i>Standard 11 – Information Communications Technology (ICT) Security: E11.110</i></p> <p><i>Standard 6 – Information Security Incident Management: E6.030</i></p>	<p><i>E11.110</i> - The organisation logs system events and actively monitors these to detect potential security issues (e.g. intrusion detection/prevention systems (IDS/IPS)).</p> <p><i>E6.030</i> - The organisation's information security incident management processes and plan(s) contain the five phases of:</p> <ul style="list-style-type: none"> Plan and prepare; Detect and report; Assess and decide; Respond (contain, eradicate, recover, notify); and Lessons learnt.
7	Providing input into personnel backgrounds.	<p>Just as appropriate screening and vetting should take place during the hiring of personnel, providing appropriate input when personnel leave is also critical to ensure that suitable visibility is provided to potential employers within the public sector.</p> <p><i>Standard 10 – Personnel Security: E10.030</i></p>	<p><i>E10.030</i> - The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.</p>

Flag	Issue	Control considerations	Element reference
8	Following off-boarding procedures upon departure of personnel.	<p>Ensuring that the full life cycle of user access (physical and logical) is appropriately managed – especially de-provisioning for when a user leaves the organisation. This is critical for preventing future unauthorised access.</p> <p><i>Standard 4 – Information Access:</i> <i>E4.050</i></p> <p><i>Standard 10 – Personnel Security:</i> <i>E10.050</i></p>	<p><i>E4.050</i> - The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes.</p> <p><i>E10.050</i> - The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.</p>

Suggested next steps

Implementation or uplift of controls covering:

- **Personnel security** – ensuring appropriate personnel security screening measures are in place and personnel are managed throughout their engagement with the organisation all the way to departure;
- **Information security obligations** – ensuring that risk centric security awareness and training is conducted on a regular basis and that personnel feel safe to “speak up” if they notice potential suspicious events;
- **Information access** – ensuring that roles and permissions are appropriately assigned and reviewed on a regular basis. When user access is no longer required, it should be deprovisioned within an appropriate timeframe;
- **Logging and monitoring** – ensuring that appropriate use cases are defined to identify potentially suspicious/abnormal user behaviour. Ensure it is recorded in a manner that it can be used (if necessary) to support appropriate incident management; and
- **Information security incident management** – ensuring appropriate incident detection and response processes and plans are in place.

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

This case study does not constitute legal advice and should not be used as a substitute for applying the provisions of the Privacy and Data Protection Act 2014, or any other legal requirement, to individual cases.

Please note that the events depicted in this case study are based on actual events, however the characters are purely fictional and any similarity to any person living or dead is merely coincidental.