11-30-2010

Information Security Disclosure: A Victorian Case Study

Ian Rosewall
Deakin University

Matthew Warren
Deakin University

Recommended Citation

Rosewall, I., & Warren, M. (2010). Information Security Disclosure: A Victorian Case Study. DOI: https://doi.org/10.4225/75/57b6762334786

DOI: 10.4225/75/57b6762334786
8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Information Security Disclosure: A Victorian Case Study

Ian Rosewall and Matthew Warren
School of Information Systems
Deakin University
Melbourne, Australia.
ian.rosewall@deakin.edu.au
matthew.warren@deakin.edu.au

Abstract

This paper will focus upon the impact of Generation Y and their attitudes to security. The paper will be based around discussing the findings of a recent report by the Office of Police Integrity (OPI) on "Information Security and the Victoria Police State Surveillance Unit".

Issues that will be discussed include the context of Generation Y and how they contribute to the case study, their attitudes, or their perceived attitudes to security of information. A discussion of the OPI report itself, and the issues that have arisen. A brief overview of the key findings within this report and the implications of these findings.

Keywords

Security, Information disclosure and Information Society.

INTRODUCTION

In today's society Information can be considered to be an extremely valuable asset to any company or organisation. None more so than any organisation that serves the general public such as, the military or the police force, or for that matter, any public service as these are privy to sensitive information about all of us. The focus of this paper is the Victorian Police and recent disclosures that have proved to be fatal for some of those whose information has been disclosed, but more importantly the change of attitudes towards sensitive information.

This paper examines the report by the Office of Police Integrity (OPI) Victoria "Information Security and the Victorian Police State Surveillance Unit" (OPI, 2010) which was published and presented to the President of the Legislative Council and the speaker of the legislative Assembly, in February 2010.

BACKGROUND

The Victorian police have had a chequered past and unauthorised Information disclosure has featured prominently in their recent history. The cases that will be alluded to, are not used in order to apportion blame but, rather to illuminate certain areas of the various reports that have been cited in this paper. As far back as 2003 Victorian Police review finds " ...inconsistent and inadequate approach to data Management" (Mc Kenzie 2009).

Data management was also blamed for the Murder of Terence Hodson and his wife in May 2004. Investigations which led to the arrest of Rodney Charles Collins in June 2008 found that he had his own surveillance dossier. When questioned on the matter he claimed that he had found them at a bus stop (Gary 2008). Collins is also 'a person of interest' for the murder of Hodson, a police informant and his wife.

Further allegations from prominent people were directed at the Surveillance unit and their management of the Hodson files in particular, Tony Fitzgerald QC in his January 2005 report found that the system in place was "grossly inadequate"

The "Investigation into Victoria Police's Management and Law Enforcement Assistance Program (LEAP)" was highly critical of the systems in place and found there to be "chronic failings' (McKenzie, 2009). Confirmation that several of the reported leaks have been traced back to the forces Surveillance team has been highlighted by a damning article in 'The Australian' newspaper "The force revealed yesterday that details from at least two secret dossiers on targeted criminals had been leaked to underworld figures from the force's covert surveillance unit." (Gary 2008).

Ironically, amidst all of these allegations against the surveillance unit, an article in 'The Age' suggests that Information about the surveillance Officers themselves has gone missing. "The loss of the documents has infuriated surveillance Police, who hold concerns that their names and confidential details could fall into the wrong hands. Surveillance Police work in a top secret environment- most do not disclose the nature of their work to other Police, family members or friends" (McKenzie 2009)

The context (Generation Y)

Many papers have been written about Generation Y (Gen Y), about their perspective on Information and the sharing of that information. Generation Y are defined as those born between 1982 – 2000 according to McCrindle (2010).

.Typically, Gen Y is your twenty-something-year-old employee who is, at this point, likely be engaged as a graduate, associate or in a support role within the workplace. This demographic is tech-savvy and engaging, and reminds other generations that workplaces can, and should, be fun. The flipside is that Gen Y has been criticised as being short on skills, demanding, impertinent and disloyal. They often appear to have a blatant disregard for, or maybe a lack of understanding of, rank and file, and tend to question tradition. Gen Y is unafraid to challenge the organisational establishment (Williams, 2010). Descriptions of Generation Y are wide and plentiful, the search to 'pigeon hole' them continues to this day, each trying to show a different perspective. For the purposes of this paper, Williams's depiction seems to encapsulate most people's views quite well, although not definitive it provides a wide enough view to use within the confines of this paper

Several academic papers suggest that Generation Y, apart from their 'Tech Savvy' approach to sharing their personal and private information through "Facebook", "Twitter" and other social networking have an Ignorance of, or a disregard for, Information security. Further to the description above comes some worrying statistics from Garretson (2007) that would appear to enhance this perception of Generation Y.

Companies that believe they have communicated their policies sufficiently might need to think again. According to a survey done by security vendor Senforce last March, 73% of the 308 respondents said they store corporate data on removable media, and 46% said they did not have — or were unaware of — corporate security policies that protect that information (Garretson, 2007).

The following discussion will investigate (possible) relationships between what has happened in the Victorian Police Force, the emergence of a new breed of Police Officer from the era of Generation Y and the authors of the report mentioned above who, most probably, because of seniority are unlikely to have been born in the same era.

ANALYSIS OF REPORT

The following represents a brief analysis, with the restrictions mentioned above, of the official report; "The Office of Police Integrity (OPI) Victoria "Information Security and the Victorian Police State Surveillance Unit" which was published and presented to the President of the Legislative Council and the speaker of the Victorian legislative Assembly, in February 2010".

The report (OPI, 2010) is damning of the lack of control of information within the Victorian Police Force, in particular of the surveillance unit. It highlights that 'they' (surveillance unit) failed to comply with the "Commissioner for Law Enforcement Data Security (July 2007)" or CLEDS standards and several other Policies and procedures of the Victorian Police. In addition that they posed a "significant risk" in Information security for far too long. It goes on to say that there was a failure to 'adhere to protocols' when the Information was on a need to know basis, moreover that it was being negligent in its classification of this information, giving rise to large amounts of sensitive material being e-mailed without knowledge of the authorisation of the recipient. In furtherance to this the recipients, Managers, Team leaders and Operatives failed to accept that the information being forwarded to them was unauthorised and in some cases unnecessary and inappropriate. The report suggests that staff that were feeding the information "….. did not know what to exclude from a surveillance request, so they included everything" In an effort to solve this issue an Internal review (June 2009) "…. Left field operatives dangerously short of the Information needed" recently another interim solution has been implemented to alleviate these issues.

The report accepts that as a result of this investigation there is a need to establish a new governance framework. Up to the date of the report the surveillance unit has still not operated "to the standard expected of contemporary police managers". At no point in this report, is there any recognition that some of the issues that have arisen might have its roots in the attitudes of the upcoming generation. The key findings that have been released to the public are as follows.

KEY FINDINGS

The following is based upon an assessment of the "Information Security and the Victorian Police State Surveillance Unit report (OPI, 2010):

1. The State Surveillance Unit of Victoria Police (the Unit) has taken steps to improve information security practices since mid 2008. However, to date, improvements lack a robust governance and risk management framework and a commitment to implementing the CLEDS Standards.
2. Until recently, Unit Instructions were prescriptive and provided inadequate practical guidance relating to effective information security systems.
3. Until recently, Victoria Police corporate information management leadership and technological support were deficient. As a result the Surveillance Unit had a 'go it alone' attitude, resulting in stand-alone systems.
4. Surveillance operatives are fundamentally sound at gathering information, but their practices in the storage, use and dissemination of that information are, at times, flawed.
5. Managers and leaders within the Unit have been focused on achieving operational outcomes and have neglected administrative and accountability processes.
6. Managers and leaders within the Unit have relied on past experience without embracing change and improving practices and information handling processes.
7. Information and intelligence provided to the Unit from investigators are not in a consistent format and Requests for Surveillance continue to contain large amounts of inappropriate material.
8. Until recently, the Unit's Intelligence Cell operated as an under-resourced information management centre rather than as a dynamic intelligence analysis unit providing support to operatives.
9. The Surveillance Unit currently uses Victoria Police's intelligence and investigation system Interpose as a document management system and under-utilises its capacity to manage intelligence, analysis and information dissemination.
10. Inadequate formal attention is paid to risk management or the assessment of current practices with a view to continuous improvement.

DISCUSSION OF KEY FINDINGS

The following is a discussion of the key findings of the "Information Security and the Victorian Police State Surveillance Unit report (OPI, 2010):

1) *The State Surveillance Unit of Victoria Police (the Unit) has taken steps to improve information security practices since mid 2008. However, to date, improvements lack a robust governance and risk management framework and a commitment to implementing the CLEDS Standards.*

The report highlights severe cracks in the expected procedures not least, that there was only one person within the team who had formal clearance which would match the standards set out for and by Commonwealth Government. Further to this there "..was some doubt as to the validity of that vetting, particularly in relation to the Australian Government Requirements" As with most civil service departments the emphasis for the solution is more 'frameworks' and more 'governance' putting aside the fact that the current frameworks and governance procedures are not being adhered to., then why expect new frameworks and governance to be more readily acceptable.

"Anecdotal evidence would suggest that these modern working practises has produced a decline in the security at department level and more disturbingly at a personal level. Burton goes on to say that ".... the younger generation of MOD staff are not inculcated with the same culture of protecting Information as their counterparts from previous generations." Alluding of course, to the 'cold war' era, where Information security was of paramount importance" Rosewall & Warren (2009).

Frameworks and the governance should be clearly defined and live within the confines of the task they serve to monitor. The modern Generation Y do not accept instructions per se rather, they have been taught to question everything. Whilst this is highly commendable in some aspects of Police work there are other areas that have to be written in stone. The handling of the Gen Y attitudes is nothing more difficult than to clarify why these actions must be followed. Hansen

(2010) suggests that: "Generation Y workers should learn to choose battles carefully, not question every single decision made, and give employers a chance to adapt to their style of work".

2) *Until recently, Unit Instructions were prescriptive and provided inadequate practical guidance relating to effective information security systems*.

Again this finding highlights the 'if you just tell people, it will happen' attitude to leadership.

We need to accept that there has been a significant change within the culture of the workplace, whereby we now live in an environment where fast and often uncensored exchange of Information is normal. In a police force environment behaviour like this in the workplace, could be devastating. Burton (2008) suggests that this behaviour should be "tempered by common sense and sound judgement" he also rules out the possibility of returning to the paper systems and thinking of fifteen years ago, arguing that cannot be considered practical in the modern working environment". It would appear from the content of this review that little or no time is spent, on the subject of information security and several examples of physical security breaches (Loss of laptop that held detailed information was stolen from a car) have had little attention paid to them.

What is really interesting in the review, is the staff's perception of Information security and how they personally, view their interaction with it. Despite the array of severe breaches of security that have been highlighted here they (the staff) appear to be happy with the current position.

The staff survey shows for example, when asked the question "Individual SSU operatives exhibit high information security awareness at all times" a result of nearly 90% felt that they either agreed or strongly agreed that this was the case, and 93% felt that their team leader sets a positive example for the secure handling of information and SSU assets.

3) *Until recently, Victoria Police corporate information management leadership and technological support were deficient. As a result the Surveillance Unit had a 'go it alone' attitude, resulting in stand-alone systems.*

This finding has little to do with the staff per se but rather that the staff that were available to the unit were insufficient and undertrained. The staff involved seemed to try to 'make the best of a bad job'. These finding are not a reflection of the attempts to do the job but rather, a situation that appears to be prevalent in any not for profit organisation. The report was damning of the attitudes of staff but also accepting that the unit reflected a lack of information security awareness which could point to the lack of appropriate training and or understanding of how information security should be conducted.

4) *Surveillance operatives are fundamentally sound at gathering information, but their practices in the storage, use and dissemination of that information are, at times, flawed.*

This rather sweeping statement appears to be based in fact when it is set against the examples given previously of gross misconduct within the unit in regards to the amount of information that has become available to the general public by, either leaks, or poor handling abilities of the staff of the SSU. However when the question was asked in the staff survey "I clearly understand Victoria Police information security policies and procedures regarding acceptable use/handling of information" 71% were quite sure that they understood what was expected of them. What is alarming here is that 29%, nearly a third of those questioned either didn't know or actually disagreed with the statement. Yet when the question posed changed it's context to "I clearly understand my responsibilities for handling and safeguarding information" 93% of staff moved to the right of the Likert scale. This could suggest that although they clearly understand what is expected they either disregard it or believe that they were correct not to adhere to it on this occasion.

This relates to the view that "While some people refer to this cohort of people as Generation Why for a reason, it is not so much an issue of a lack of respect for authority as much as it is that this group has been raised by their parents to question everything and raise questions when they don't understand something. This generation is very independent and not afraid to challenge the status-quo. Many in Generation Y want a relationship with their boss like the ones they have with their parents. It's not that these folks have little respect for authority; on the contrary, they feel employers do not respect them." (Hanson 2010)

Perhaps, the statistics in this case may add to Hanson's perspective and extend his point of view to, that if Gen Y do not agree with something they have been told without explanation, that they will simply ignore it.

5) *Managers and leaders within the Unit have been focused on achieving operational outcomes and have neglected administrative and accountability processes.*

"The modern position of "Need to Share" leads to "unacceptable vulnerabilities". Accepting this situation means that working practises within the MOD need to be reviewed without ignoring the benefits of the new emerging technologies and yet still being vigilant with regards to Information security."(Rosewall & Warren 2009)

Although Rosewall and Warren are discussing the UK's Ministry of Defence (MOD) the relevance is clear. This need to focus on the outcome and not on the means, reveals 'unacceptable vulnerabilities'. In the case of the Victorian Police it is alleged that this attitude caused the death of at least one person. A key view could be "....police do not exercise legislative power; that is to say, they do not make laws. This observation may seem trite, but its implications are sometimes overlooked. Less obvious, but equally important is the need to guard against vesting in the police discretionary powers which, for practical purposes, may amount to powers to make law, or to dispense with the compliance with the law." (Gleeson 2010)

It could be argued that taking more care over administrative and accountability processes could also be of great value to the Victorian Police, in as much as following due process could provide evidence of accountability when cases of disclosure are aired. Several cases that have been jumped on by the press, cause more concerns when the Victorian Police seem to be unaware who leaked the information but, even more worrying is that are not sure who had the information to start with, further they cannot guarantee that those that did have the information had the right security clearance.

6) *Managers and leaders within the Unit have relied on past experience without embracing change and improving practices and information handling processes.*

On reading the report it becomes clear that there is no line of accountability within the management structure. Job descriptions do not appear to cover these duties specifically so, once again, the onus is on each individual manager to interpret the duties that they are expected to perform. Some managers have created their own checklists to try to maintain some sense of order, although this does not appear to have been filtered down the chain of command. This became evident when a large number of sicknesses amongst the management members happened, the rest of the team were clearly not equipped to deal with the situation. As described earlier this lack of clarity allows the Gen Y members of the team to find their own solutions. Technology has allowed this generation to multitask and find shortcuts in achieving tasks which may not be the most secure route. Although change can be a good thing, and should be embraced at senior management level. There is also a case for keeping the same ideology, security, but achieve it in a different way. Various accounts of unsupervised access to sensitive information and unauthorised persons obtaining this Information, is the area that needs to changed by whatever means necessary.

The example given above, absent managers, gives rise to the situation where untrained staff are required to undertake tasks that they see as boring and or unnecessary, or beyond their capabilities and without proper security training offer up the possibilities of unauthorised information disclosure on a massive scale. Although the staffs that were surveyed believe that they are up to the job it has been proved that they are not. The report identifies this aspect as gross understaffing and this does appear to be the case. This situation, since 2008 does seem to be improving, but still the 'untrained' aspect would appear to remain.

7) *Information and intelligence provided to the Unit from investigators are not in a consistent format and Requests for Surveillance continue to contain large amounts of inappropriate material.*

The report suggests that staff that were feeding the information "….. did not know what to exclude from a surveillance request, so they included everything" this on occasions, could be upwards of 100 pages and would have countless photocopies made of them with no restrictions or audit trails conducted. This practice has now ceased to a large extent.

The report identifies that there is an inherent fault in their security management that most of the information that they hold not only lacks the robustness that we, the general public, expect but also that the information that they do hold is not classified correctly, or worse still not classified at all. This was admirably demonstrated by the reports acceptance that the unit received information gleaned from telephone intercepts which it was 'not equipped' to receive or store. The unit therefore had breached statutory obligations. Which would suggest, that they were unaware of these obligation or, they chose to ignore them. This was further compounded when the report found that they had also breached the Victorian Police corporate policies on intelligence management.

Ironically, the procedure for requesting data from the unit was, initially, by phone which is generally considered to be the least used forum by Gen Y and more the preferred method of Generation X. This conversation was the basis of whether or not the request was moved on to the next stage. Gen Y are far more likely to prefer the e-mail approach which would facilitate a more formal request with some detail included and a more robust audit trail. The e-mail approach is stage two for the generation X style of request, therefore perhaps, it could be suggested that the Gen Y have the upper hand in this instance. However, once the information was released it would invariably contain much more information than was requested or for that matter, should have included. This brings us back to the 'need to know' versus 'need to share' situation was has been suggested is very much the trait of the Gen Y mentality.

8) *Until recently, the Unit's Intelligence Cell operated as an under-resourced information management centre rather than as a dynamic intelligence analysis unit providing support to operatives.*

A review conducted in 2005 found that there was a confusing array of information flows within the unit. This prompted the author of that report to suggest that, within the unit there should exist, an intelligence cell. An ad hoc cell was created which proved to be less than expected. It was poorly resourced and was staffed with individuals that were unqualified which led to a lack of direction. In this particular case, the Gen Y members would certainly be able to contribute, as they are often described as being 'technology savvy' and have the ability to think outside of the box without the history, or baggage that the Generation X staff would bring to the party. Too often the older generations would proffer the argument that "we have always done it this way". The situation within the unit obviously needed new thinking and new ways, tempered by the experience of the Generation X staff but not restrained by them.

9) *The Surveillance Unit currently uses Victoria Police's intelligence and investigation system Interpose as a document management system and under-utilises its capacity to manage intelligence, analysis and information dissemination.*

On the 1st July the unit moved to using 'Interpose' a bespoke software for the correlation and dissemination of intelligence data for use by its police force. The reservations that the report highlights, tend to allude to the operation of this system rather than blame being apportioned to the unit. Staff are required to manually enter data into the new document. Requests have been forwarded, asking for a template which could be used by staff making requests. However they have been advised, a solution is probably available but it will take a few years to develop! This again highlights areas that the new generation could be of a great advantage. In order to accept that this is possible we will need to rectify the situation, that is generally accepted namely that the attitudes of Gen Y staff in the workplace can lead to potential conflict between the different generations within the workplace. A survey by Lee Hecht Harrison found that "60% of employers experience tension between employees from different generations. This tension is often two-way with 70% of older employees dismissive of younger workers' abilities while 50% of younger employees are dismissive of older co-workers." If the Gen Y staff could solve the problems mentioned above, perhaps we could enjoy a more stable working relationship and alter some of the statistics that Harrison has put forward.

10) *Inadequate formal attention is paid to risk management or the assessment of current practices with a view to continuous improvement.*

The staff survey that was conducted, shows that the current staff are more than happy with their current state of awareness their argument lies in that they feel that the formal attention that has to be paid, 'inhibits their ability to perform their roles" and yet the survey shows that these same members of staff, or at least 89% believe that their unit fully complies with their information security responsibilities. This paradox could be the result of a poorly constructed questionnaire or, the staff's lack of what exactly is information security, which again raises the issue of understanding and training.

The report concludes that there are failures in the proper authorisation processes, 'who should receive what'. The practice of operatives and investigators exchanging information without any security controls is an issue which is likely to increase when the Gen Y start to move up the promotion ladder with their perceived 'need to share' beliefs. This was highlighted by the report's findings that the culture within the unit was one that believed that 'more information is better'.

CONCLUSION

The Victorian police have had a chequered past and unauthorised Information disclosure has featured prominently in their recent history. The cases that were highlighted, are not used in order to apportion blame but, rather to invoke discussions in this area

The paper shows the impact of organisational culture and its relation to Information Security. In regards to this paper we have focused upon the Victorian State Police in Australia and the cultural problems that they are having regards to the disclosure of Information. The paper also reviews some of the key findings put forward by the Victorian Office of Police Integrity to solve these problems.

This paper has discussed (possible) relationships between, what has happened in the Victorian Police Force and the emergence of a new breed of Police Officer from the era of Generation Y. The report is damning of the lack of control of information within the Victorian Police Force, in particular of the surveillance unit. In addition that they posed a "significant risk" in Information security for far too long. We have shown a possible failure to 'adhere to protocols' when the Information was on a need to know basis, moreover that it was being negligent in its classification of this information.

The key findings illustrate the modern position of "Need to Share" which can lead to "unacceptable vulnerabilities". Accepting this situation means that working practises within any organisation needs to be constantly reviewed without ignoring the benefits of the new emerging technologies "...and yet still being vigilant with regards to Information security."(Rosewall & Warren 2009)

It is highly probable that the Victorian Police are not suffering these issues in isolation and further research will be carried out in this area to try to ascertain if there is a pattern that can inform future decisions in this area.

REFERENCES

Burton, E (2008) Report into the Loss of MOD Personal Data, Minsitry of Defence, UK, Report accessible via: http://www.mod.uk/NR/rdonlyres/3E756D20-E762-4FC1-BAB0-08C68FDC2383/0/burton_review_rpt20080430.pdf, Accessed 15th September, 2009.

Office of Police Integrity (OPI) (2010) "Report - Information Security and the Victorian Police State Surveillance Unit", Victoria, Australia.

Gary, H (2008) 'State's force still full of leaks', The Australian, 15th August.

Garretson, G (2007) Balancing Generation Y preferences with Security, Network World, August, URL: :http://www.networkworld.com/news/2007/082907-security-standard-5.html?page=2, Accessed 1st September, 2010.

Gleeson A (2010) Police Accountability and Oversight: An Overview, UR: http://www.walk.com.au/pedestriancouncil/Page.asp?PageID=339, Accessed 1st September, 2010.

Hansen, R (2010) Perception vs. Reality: 10 Truths About The Generation Y Workforce, URL: http://www.quintcareers.com/Gen-Y_workforce.html, Accessed 1st September, 2010.

Mc Kenzie, N (2009) 'Watchdog's report damns police over leaked files - 'Systemic failure' to manage data', The Age, 16th October.

McCrindle, M (2010) Understanding Gen Y, URL: http://www.learningtolearn.sa.edu.au/Colleagues/files/links/UnderstandingGenY.pdf , Accessed 1st September, 2010.

Rosewall, I. and Warren, M. J. (2009) Information security disclosure : a case study, Proceedings of 7th Australian Information Security Management Conference, pp. 39-47, Edith Cowan University, Perth, W.A.

SmartManager (2010) Getting Workplace Value from Generation Y, URL: http://www.smartmanager.com.au/web/au/smartmanager/en/pages/87_workplace_value_gen_y.html, Accessed 1st September, 2010.

Williams, K (2010) Understanding Generation Y, URL: www.dynamicbusiness.com.au/.../understanding-generation-y.html, Accessed 1st September, 2010.