Copy 1 of 1

CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

CONDUCTED AT LEVEL 2, NORTH TOWER, 515 ST PAULS TERRACE, FORTITUDE VALLEY WITH RESPECT TO

File No: CO-19-1209

OPERATION IMPALA
HEARING NO: 19-0006

DAY 1 - MONDAY 11 NOVEMBER 2019
(DURATION: 0HRS 38MINS)

Copies of this transcript must not be made or distributed except in accordance with any order made by the presiding officer concerning publication of these proceedings.

LEGEND

PO Presiding Officer – ALAN MACSPORRAN QC
CA Counsel Assisting – JULIE FOTHERINGHAM
HRO Hearing Room Orderly – KELLY ANDERSON
W Witness – RUSSELL SMITH
LR Legal Representative – N/A

HRO All stand.

PO Thank you. Be seated. Yes, Ms FOTHERINGHAM.

CA Thank you, Chair. I call Professor Russell SMITH.

W Good afternoon.

PO Good afternoon. How are you? Do you prefer an oath or after mission?

W I will have an oath. Yes.

PO Yes, we will swear you in. Thank you.

HRO UI and repeat after me. The evidence which I shall give.

W The evidence which I shall give.

HRO In these proceedings.

W In these proceedings.

HRO Shall be the truth.

W Shall be the truth.

HRO The whole truth.

W The whole truth.

HRO And nothing but the truth.

W And nothing but the truth.

HRO So help me God.

W So help me God.

HRO Thank you. Take a seat.

PO Yes.

CA Thank you, Chair. Good afternoon, Professor SMITH.

W Good afternoon.

CA Can you just state your occupation for the record?

W Yes, I'm a principal criminologist at the Australian Institute of Criminology in Canberra.

CA And your main areas of expertise are?

W It is economic crime generally, with a focus on cybercrime, financial crime fraud and corruption prevention.

CA Thank you. You have qualifications in law psychology and criminology from the University of Melbourne and a PhD from King's College, London. Could you elaborate on those qualifications?

W That's correct. I practised as a lawyer for a number of years, and then undertook some postgraduate study in London where I did research on medical misconduct, and then taught at the university for a couple of years and then took up a position in Canberra at the Australian Institute of Criminology, where I've been for about 25 years.

CA And you have published several - there's several publications that you have in the area to which we are interested in.

W Yes. Yes, many publications on corruption prevention and economic crime, 400 or so.

CA There's the Cybercriminals on Trial and Economic – Electronic theft.

W Yes, they're two cybercrime specific works which looked at the problem of information misuse in the public sector and in other contexts.

CA And also Crime in the Digital Age.

W Yes, that looked at a sample of convicted offenders internationally who'd committed cybercrimes essentially to compare punishments imposed on them.

CA And Cybercrime Risks and Responses Eastern and Western Perspectives.

W Yes, that was another cybercrime work written with some collaborators in Hong Kong that tried to compare how eastern and western countries were approaching the problem of cybercrime, particularly in the sentencing aspects.

CA And you are a fellow and former president of the Australian and New Zealand Society Of Criminology.

W Yes, that's correct.

CA And the former president of the Asia Pacific Association of Technology and Society?

W Yes, correct.

CA And just lastly, in 2014 you were appointed as adviser to the Victorian Law Reform Commissions inquiry into the use of regulatory regimes to help prevent organised crime and criminal organisations?

W Yes, that's correct.

CA Thank you. And you were provided an attendance notice today?

W I have received that, yes.

CA Can that just be shown, the notice?

W That's the notice, yes.

CA I tender that notice.

PO Make that Exhibit 14, thank you.

ADMITTED AND MARKED EXHIBIT 14.

CA In relation to the area of education, with a view to preventing misuse of information within the public sector agencies, what is your view in relation to privacy awareness campaigns?

W I think they're part of a general package of anti-corruption measures that are used. Unfortunately they haven't been evaluated effectively almost anywhere in the world. There's anecdotal examples in some countries where campaigns have been attempted to be evaluated but they haven't been terribly effective. Part of the reason for that is that usually campaigns like that are introduced at the same time as other initiatives to deal with a corruption problem, and so it is very difficult to disaggregate the effects of the campaign itself as opposed to the other more general measures. For example, if you set up an anti-corruption commission in a country, and as part of that introduced an education campaign to try and raise awareness of the problems and educate the community, it is difficult to know what effects are due to the education initiative as opposed to the other activities of the new anti-corruption commission. There have-

CA -Sorry.

W There have been one or two examples of evaluations but they both suffer from those problems. And I could provide references to those if the Commission is interested.

CA If you can name a reference, yes.

W Yes. There's one by an author Berry in 2012 in the Journal of Business Ethics which looked at the impact of ethics programs in particular. Another one by Professor Rose Hearn, looking at the role of education in changing corrupt practices. And that's looked at education initiatives more generally.

CA For awareness campaigns to have effect, in your view, how regularly should they be rolled out, as it were?

W They should be available to staff in the public sector from their very start, from the commencement of the people. So when people join in the organisation they should be made aware of the policies and principles that are in place to deal with misuse of information. And then depending on the nature of the risks involved, so whether they are particularly serious, or if they have very, you know, demonstrable potential consequences, then more regular reinforcement of those education measures would be needed.

CA Are you speaking specifically about training as opposed to an awareness campaign?

W Yes, I would think both actually.

CA And should the training courses be in-person or online?

W Probably a mixture of both. Although, arguably there would be more direct impact on an individual if they're asked to sit through a face-to-face session, you know, for an hour or an afternoon as opposed to working through a series of tasks online. But it's often beyond the resources of some organisations to have face-to-face sessions. It is sometimes so expensive or too administratively difficult to do that.

CA You said, Professor, that the training courses, I'm just speaking about training courses at the moment, say a module, should be onboard, so when there's an induction and then the frequency should be based on the level of risk pertinent to the misuse of information. Is that the risk of any consequences that may flow from the misuse of that information?

W Yes.

CA In the instance of a domestic violence victim, the consequences would be much more so than someone who wasn't a domestic violence victim and had their information disclosed?

W Yes. Yes, definitely. There's some cases where risk of death could occur. For example, if a human source, an intelligence agency's identity was revealed then that would be a very direct risk of death resulting from misuse of information.

CA So when you talk about high risk you're talking about physical danger for the victim of the misuse?

W There's a variety of consequences. They could be substantial economic harms, which could result in, you know, loss of a business and/or the employment of the staff through to personal harms, violence against individuals. Or misuse that could take place in health settings where medical records are altered or manipulated in some way or information is leaked to an insurer, for example. In those situations then there could be again personal, physical and emotional harm as a result of that.

CA With the high-risk situations that you've just covered some of the range of categories, how often should the training occur?

W I would think there would need to be at least yearly or two-yearly overall refresher programs.

CA When you mean overall, is that for any level of risk?

W For all of the people-

CA Yes.

W -who might be at risk of misusing information.

CA And for the high-risk category?

W For high-risk potentially more frequent, but I'd suggest that it's probably dependent on the particular risks that that individual or that group of individuals are facing. So, for example, if there was a new risk identified in an organisation that would require the staff to be trained to deal with that, then that would be appropriate to have a new training program. It might not be necessary to have it regularly if there's no change in the overall range of risks that are present.

CA Should the training be relevant to the role?

W Yes, definitely. The people who are receiving the training are very unlikely to make use of it if it is not relevant to their daily work and interests. And it is part of the problem with many training programs is that they are sometimes too broad and not targeted on individuals. And it is likely that they are going to become mundane in those people's lives and they really won't take up the important messages that are being provided.

CA What is your view in relation to a daily log-on warning prior to access to the database?

W Again, I think that's useful, as long as it doesn't become mundane for the

people who are seeing it. So I know in my own organisation there's security messages that are on the desktop, and over time they don't change and you lose the importance of the message. If those types of messages are changed regularly and particularly to account for change in circumstances; for example, in Queensland we have bush fires at the moment. If you had messages that are appropriate for that risk situation, then people are much more likely to take an interest in them and alter their behaviour.

CA And would it prove more effective if on a regular basis there was an assessment part to the warning prior to being able to access?

W Yes, definitely. Any training programs or education initiatives should be evaluated, both so that the individual who's receiving them has satisfied some measures of having understood them, and also to see whether their messages are actually targeting the outcomes that they're trying to achieve.

CA Are online updates a valuable preventative tool?

W Online updates are useful as long as there's not too many of them and they don't overwhelm the readers. So they need to be very specific and targeted and not over-used. And they also need to have accurate information. If information is being provided that people know is not quite right or out of date then they're going to lose confidence in the messages.

CA How often should the updates be rolled out?

W I would think a general 12-monthly review would be useful if the organisations have got the resources to undertake that research and to do the alterations necessary. But if there's a specific change in the circumstances in which the organisation's working, then there should be an update as soon as possible.

CA In relation specifically to information privacy training around the misuse of information by public sector employees, should that be mandatory training?

W Yes. Yes, I would think so. Yes.

CA And should all training, whether it be in-person or online, be assessed at the end of it?

W Yes. Yes, definitely.

CA In relation to policies, should they be consistent across all public sector agencies?

W I think the overwhelming general principles that they're trying to achieve should be, you know, form – and ideally across Australia, not within States and Territories, and ideally aligning with Commonwealth interests as well so

that we have a uniform set of principles that people can adhere to. But they need to be focused on the particular circumstances of the organisation that's sending them out. So, they need to be more specific than the very general principles but still follow those overall guidelines.

CA Should they be simple?

W Yes, as simple as possible. As we all know, some of the fine print in online messages that we receive and contracts are just far too detailed to be able to be read easily and effectively and people will usually ignore them. And there's research that supports that, that people just don't understand or have the time to soak up 30 or 40 pages of detailed information. If you have a single page with highlighted, very specific messages, then people probably will understand it and make use of it.

CA And should there be an effort on behalf of the agency to consolidate similar policies into one document?

W Yes, yes. If there's an employee who's working in different fields, with different interests, and there are separate policies that govern each of those different work policies, then they should be aligned as much as possible.

CA And specific to the information privacy for the misuse of information, a policy for that, should that include clear advice in relation to the entire range of disciplinary and criminal penalties that would flow potentially from the misuse?

W Yes, it is important to have the range of sanctions available to people, although, again, research has found that people often don't believe that they're going to be applied to them individually. It's very difficult to make people understand that a range of potential sanctions will eventually be applied to them if they do the wrong thing. So ways around that problem are to demonstrate cases where sanctions have been applied, case studies where cases have gone to court, people have received terms of imprisonment or serious fines, and people can then see that the sanctions are in fact applied. Simply having a list of available penalties probably isn't going to make that much impact on people.

CA If an agency does in fact have a case study, as you have just spoken about, in their policy, or sending them by way of a newsletter on a regular basis, and the case studies or case study in particular shows that there is a very light disciplinary outcome, then what would that - what affect would that have on the culture of the organisation?

W I think if the detail of the case is explained carefully, then people understand that this – that particular case might not have been the most serious, and the various aggravating and mitigating factors that have been taken into account are understandable. If it is simply presented as someone hacking into a

computer network and taking data and they received a $2,000 fine without further explanation then that might trivialise that act. But if it is explained in much more detail and you actually understand what was involved and the personal circumstances of the individuals, as in any sentencing situation then I think the community will understand it.

CA And if I could just show you an article, a Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse Among Unsworn Police Employees, a report by Nikki Rajakaruna, Pamela J Henry and Adrian Scott from 2018, pages 1 to 3, and I have the entire article for you as well. And I tender pages 1 and 3.

PO I'll make that Exhibit 15, thank you.

ADMITTED AND MARKED EXHIBIT 15.

CA If we just turn to page 3, the second paragraph that starts with "A basic deterrent strategy".

W Yes.

CA In the article the basic deterrent strategy is said to be best if it outlines appropriate and inappropriate behaviour and it enables employees to place parameters around their behaviour, ensuring that they behave in accordance with agency expectations. Is that best practice to include that type of detail in specific policies to prevent misuse of information?

W Yes, yes. Basic principles of deterrence involve knowledge about the certainty of being detected in terms of illegality and also understanding the potential sanctions that might be involved. This particular article found interestingly that it was the perception of the overall punishment was more important than simple detection, which is contrary to some other research, but I think it is nonetheless a useful finding.

CA And in that same paragraph , they also talk about policy should increase the awareness of the negative consequences as you've just said.

W Yes, yes.

CA But the presence of policy itself is unlikely to deter misuse of information if there isn't awareness of the consequences which you've just UI-

W Yes.

CA Now, how often should public sector employees be exposed to the policy for it to be effective?

W Well, as I said before, I think without oversaturating people with information

that they already know, it is important to refresh the message regularly, you know, perhaps every one or two years depending on the circumstances. But to have constant reminders probably dilutes the effectiveness of it.

CA The article talks about single exposure not being sufficient.

W Certainly one exposure which happens in many workplaces as soon as a person is engaged in the organisation they are given packages of policies and information, and then that's never refreshed and often we'll see people who have been in an organisation for 15 to 20 years who have no refresher courses or information at all, and they're the ones who are often at risk of committing frauds or misconduct or dealing with information incorrectly when the circumstances are correct.

PO I suppose, Professor, one way of refreshing the policy without directly referring to it is to publish de-identified case studies where action has been taken to relate it to the consequences of a breach of the policy.

W Yes, I think that's a much more effective way than having just fairly bland descriptions of what policies are, which a lot of people find difficult to read.

PO And to relate to their personal circumstances particularly?

W Yes, yes.

CA In relation to the risk of misuse of information, is it the case that the greater the volume of the information held by an agency the greater the risk?

W Potentially. The risk factors depend on the probability that the misuse will take place and also the consequences that we spoke of earlier. But if you have very large amounts of information, such as those collected by large social media companies, or hospitals, or revenue agencies in countries, then the potential damage can be enormous.

CA The Department of Education and the Department of Health have a decentralised set-up where there are the schools that they have an overarching responsibility in relation to, in part, and Health there are the Hospital Health Services. In relation to the evolution of responsibility for policy and education, what responsibilities, if any, should those two departments have over their smaller agencies?

W I think partly the answer to that relates to the resourcing that different parts of an organisation have. Often smaller entities that are managed by a larger department don't have the same resources as the larger department, clearly. And so, as a result of that, there's probably a greater likelihood that a central agency can develop policies, education materials, and give information that's relevant for the whole set of devolved entities working with that department. Often the very smaller entities, such as a small school in a rural area, probably

won't have the resources to develop its own policy on information management. So the best solution is probably for departments to have templates put in place which show the range of policies and information, and then they can be adapted more easily by smaller devolved entities within the department to suit their own needs. But they probably won't be able to have the resources to do it themselves, just in terms of staffing who are knowledgeable about how to do that, and also the, you know, the time and expenses involved.

CA So best practice would be in relation to policy for there to be prescriptive templates that are provided to the smaller entities so they can follow-

W Yes.

CA -a similar path and be consistent across the entire department and smaller agencies?

W Yes. Ideally with some guidelines about how they can be adapted easily to the individual circumstances of the smaller department.

CA And on that same vein, should there be some direction and assistance with the type of education, that should be held at the smaller entities by the department?

W Yes, yes. There should be some monitoring by the central agency about what's taking place so that you don't have a smaller part of the department preparing its own material that is slightly incorrect or doesn't follow the general principles that have been outlined.

CA There should be consistency in relation to education as well as policy?

W Yes, yes.

CA I'll just show you a paper written by yourself entitled Trends and Issues in Crime and Criminal Justice from the Australian Institute of Criminology, number 534 of February 2017.

W Yes.

CA And I tender pages 1 and 13 of that document.

PO Exhibit 16. Thank you.

ADMITTED AND MARKED EXHIBIT 16.

CA You wrote this, Professor, with two of your colleagues?

W That's correct, yes. Yes.

CA And if I could just take you to the page 13, the conclusions. This is a much condensed version of a larger report, is it?

W Yes. Yes, it was a report that we – the Australian Institute of Criminology prepared for the Australian Criminal Intelligence Commission which is specifically looking at the problem of organised crime infiltration of public sector agencies. So this is a snapshot of the material that was suitable for public release and just outlines the main ideas and conclusions of the research.

CA If I could just go through the pertinent conclusions and then just trace back through the reasons for them. Number 2, that there are risks – corruption of public officials in Australia is largely anecdotal but overseas research clearly indicates various kinds of risk. And the second type of risk is risks to frontline agencies such as police. Could you expand on that?

W Yes, I think police, I also mentioned border control agencies-

CA We are dealing here with police.

W Yes.

CA Corrective Services.

W Yes.

CA Health, education and transport and main roads.

W Yes. Well, each of those have similar risks in this regard. Dealing with police, I think the main problem in terms of the organised crime infiltration aspect is that police hold a great deal of sensitive information about ongoing investigations, the resources that they're giving to particular crime problems in the community, and if that information is made available to criminals, particularly those in organised crime groups then that's particularly valuable in enabling them to tailor their activities to avoid detection perhaps to target particular areas of crime that aren't being focused on by law enforcement. And also to obtain information about people within government departments who could be easily corrupted.

CA And in that recommendation, conclusion, there's also agencies with extensive personal data holdings and decision-making functions of value.

W Yes. Where there's decision-making that might be valuable to an organised crime group, such as planning applications, anything to do with revenue collection, drug policy/activities, those type of things where decisions are made that could be useful to organised crime, then they're likely to be targeted. And so if any of those agencies have data holdings that could be relevant, that type of decision-making, then that would be useful.

CA Just going back to page 6 where you talk about the risk factors for Australia for public officials being vulnerable to corruption, the first risk you identify are motivations and benefits; namely, the financial benefit. Could you elaborate on that?

W Yes, most of our research has identified direct economic gains, greed by individuals as the primary motivating factor in most serious crime and serious and organised crime in Australia. So where there's information that are held by government departments that could result in some financial benefit, then that's a very direct motivation for people to try and obtain information illegally.

CA And the third risk is lifestyle, such as drug use, you've mentioned here.

W Yes, those drug use are the types of leisure activities that people engage in, use of social media. Those things are important in enabling criminals to establish relationships with people in sensitive positions. Often they might attend the same fitness gyms or places where drug dealings take place, and over time they can establish a relationship that can then be abused to enable pressure to be placed on a public servant to act illegally.

CA And the next risk identified are relationships. We're talking about declarable interests and conflict of interests within the public sector.

W Yes.

CA Any particular agencies out of the ones that I've talked about-

W I think the relationships I meant there were extending from familial relationships, so where public servants have family members who might be involved in criminal activities and they make use of those connections. That can often create risks. And similarly where there's business involvement. So if a public servant has a business relationship either personally or with their family member, a spouse, for example, and that involves people who are willing to act illegally in the community, either in a business sense or in some other commercial way, then that can create risks of misuse of information.

CA And then under organisational risk factors, down the bottom of that section you mention that there is a need for education to ensure a resistance to corruption, which we've already talked about.

W Yes, just having effective policies in place and organisation and awareness of risks and also some willingness by senior management and CEOs and organisations to require staff to adhere to those policies. So there needs to be direction from upper management to make sure that policies are being used, understood and applied.

CA And then under the heading "Best Practice Responses", you identify there is a need for agencies to identify at-risk employees and talk about using data analytics – advanced analytics.

W Yes. To some extent those technological tools can be very useful in identifying some risks, but there's a problem in making them too extensive and too invasive on individuals' privacies. So you need to balance personal and privacy interests with the ability to obtain information that might be relevant to potential criminality. So I think that is dependent on those who are making use of those data analytical tools being aware of the privacy and other protections that are available in legislation and making sure that they comply with them, and that's where you need external supervision to make sure that data analytics aren't being used too extensively and too invasively.

CA Thank you. Thank you, Chair, I don't have any more questions.

PO Thank you, Ms FOTHERINGHAM. Professor SMITH, thanks very much for coming. Do you want Professor SMITH excused?

CA Yes, thank you.

PO Thank you again for your time.

W Thank you.

END OF SESSION