Crime and Corruption Commission
QUEENSLAND

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 5 - FRIDAY 15 NOVEMBER 2019
(DURATION: 22 MINS)

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 – MATTHEW BELL
LR	Legal Representative – N/A

HRO All rise. This hearing has resumed.

PO Thank you.

CA Good afternoon, Chair. I call Senior Sergeant, Matthew BELL.

PO Good afternoon, Sergeant.

W How are you?

PO Do you prefer an oath or affirmation?

W Oath, thanks.

HRO 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.

CA Good afternoon, Senior Sergeant.

W Good afternoon.

CA Were you provided with a notice to attend this afternoon?

W I was.

CA May Senior Sergeant be shown the notice?

W Yes, thanks.

CA I tender that document.

PO Exhibit 83.

ADMITTED AND MARKED EXHIBIT 83.

CA Senior Sergeant you're employed with the Victorian Police Service?

W That's correct.

CA And you are the Security Operations Manager for the Protective Security, Security Information of the Privacy Division, and you've been there for six years?

W That's correct. I'm the Protective Security Operations Manager of the Security Incident Registry.

CA Could you describe the functions and staff for that area?

W Okay. The Security Incident Registry is something that was created in 2012, and it’s staffed currently by five sworn employees, and their role and function is to record, isolate, contain and consider remediation for protective security events and incidents in Victoria Police.

CA Thank you. And there's four domains the command covers?

W Yes, that's correct. So Protective Security covers information security, IT security, physical security, and personnel security.

CA Is VicPol concerned with machine learning in the information technology area?

W That's a future State. At the moment we've got a requirements document going up to find an IT solution for a machine learning for proactive monitoring.

CA And currently, what is the process for your proactive monitoring?

W At the moment our proactive monitoring is a manual process based on used cases of vulnerabilities and opportunities that have been exploited. And we use analysts and other software at the moment to detect exceptions.

CA Could you explain how those exceptions are detected?

W It is usually based on user case. So incidents that we have had through the Security Incident Registry and we look at opportunities to prevent them from happening again. And that is something that we take a data set out of one of our systems and usually compare it against a data set from another system, and the software will spit out exceptions which is then manually interrogated.

CA And what type of exceptions can you look for?

W They're quite broad, but we might look for security classified information being externally emailed, for instance. We might look at irregular volumes of printing behaviour. We might look at irregular LEAP checks. Sorry, LEAP is our computer based system. Irregular checks within our computer systems.

CA And when you mean irregular checks within your computer system, what type of activity would you class as-

W We might look at irregular volumes. We might look at, for instance, failed attempts to login without a password reset. We might have a key set of tags within our system and people who have checked that and we might look for cases where they might not have had a lawful business reason.

CA And is there a triaging of the reports which generate from those exceptions being detected?

W Yes. So each exception is investigated at a desk top level. So that's where we will interrogate the systems that we have available to us and we'll put some operational overlay over the top of what those checks may be. If it can't be explained, ie, there's not a legitimate business reason for the check, then we will escalate to our Professional Standards Command.

CA And are some matters dealt with by local line management?

W So in the case that the exception detects someone who's employed directly by Victoria Police, each one of those will be initially triaged at our division level. If it's what we consider a low risk, the first one will be notified to local management, the second one will be escalated to Professional Standards Command. If it is not a low risk check then it will be directly reported to Professional Standards Command. If the exception is outside of Victoria Police, ie, a contractor, we might look at the local Crime Investigation Unit or we might look at the contract management.

PO Sergeant what do you term a low risk access?

W So we might check, identify, for instance, they might be sending information that's not security classified home, but it is still Victoria Police information, so probably sent to a personal email address. And there may be, you know, a business reason for them to do it. We've probably got other ways they could do it which would protect our information a bit better. In the event that that is security classified or sensitive, then that goes above the low risk threshold. So we have a Security Assessment Group that we discuss these type of things with. So it's more of a grey science more than a black and white line.

CA	And how quickly are the reports actioned?

W	Well one that goes directly through to Professional Standards Command, they actually have timeframes in relation to the point that it needs to be returned back with a result. We personally like a turnaround time of, you know, 10 business days if we go directly to the local area, considering sometimes the employer might be on leave or shifts.

CA	And you've had this process in place since 2014?

W	So I did an initial review of our active monitoring activities, which was in about 2015, and we agreed on an ad hoc process which developed into getting two additional staff, and they've been in place now for 12 to 18 months, so the current process has been in place for that time.

CA	And you've made substantial progress in generating more accurate exceptions during that period?

W	Yes, correct. So we did some live monitoring of the previous active monitoring activities for an eight-week period, and we compared that with an assessment of two previous years, and both came around about less than 5% accurate detections. So those ones that were, you know, escalated we deemed to be potentially not hitting the mark.

CA	And for the around the 5% detections, there were how many actual detections per year?

W	So I'd have to look at my report, but I think it was around the 500 to 550 that I reviewed to get about the 5% over the two years and plus two months I think.

CA	And then currently you're having around how many detections per year?

W	Well, it actually fluctuates Like, we might have – if I can talk to exceptions, probably because, you know, the exceptions come out of the report that we review and that's probably more accurate. We might have anywhere from 30 a month, I suppose, at the moment. And of those that get escalated, we're probably around 50 to 60% of those either get sent to the local management for further investigation, or like a please explain type of scenario or escalated to PSC for thorough investigation.

PO	What is the size of Vic Pol, how many members?

W	We have about 20,000 probably with access to our systems. That's including some contractors.

CA Currently you say there's about 30 detections a month. And what's the percentage of actual breaches? You said previously when there are about 500 to 550 detections it was about 5%.

W So if I talk to the probably the 60% that are escalated for further investigation, I would say more than 80% of those would be identified to be not for legitimate business reason. And that's probably bringing the volume down from, you know, 500-odd down to we might only escalate, you know, 15 a month. But that's only limited by our staff because of the manual process we have in place at the moment.

CA So you've managed to become a lot more efficient in generating more accurate exceptions?

W Yes, that's correct.

CA And that has reduced the amount of reports that need to be manually gone through as the assessment to whether or not it is actually a breach, or they're potential breaches?

W Yes, that's correct. So the exceptions of potential breaches.

CA Yes. So how have you managed to become more accurate in generating exceptions?

W Through used cases through the Security Incident Registry. So at the moment we're looking at 1,000 security incidents for this year. Each one of those are considered for remediation, ie, what we can do to stop it from happening again. So then we can focus the proactive monitoring on the particular trigger that could have been identified.

CA And your system is able to have flags when there's password sharing. Did you want to explain about that?

W So not so much as flags at this point, that's probably with the machine learning, but the logon events are obviously correlated and they can be down to a location where the machine is. We can put those reports into an analyst tool which can spit out where there's simultaneous use on the same system with the same user base. So that is an indication for us of password sharing. Another one may be instances where one person, one user is logged into the actual local area network, and then a second user is logged into a system on that same user account, is another indicator of password sharing.

CA And you talked about machine learning. And there's a tender ,Vic Pol currently have a tender for that software.

W Yes, so we've got a requirements report in relation to analytics over end user and behaviour in the systems, which we will probably look at in the next, you know, few months, with a couple of extra staff because it will take a long time to build the algorithms into that to identify the detections, and then we fine tune it, and then to monitor the exceptions to come out are expected to be, you know, considerably high.

CA Could you explain the difference between machine learning and artificial intelligence?

W I can try. I'm not a specialist in that field. My understanding is that machine learning is basically a type of AI. Machine learning is one where we tell it what to look for. And based on, you know, what it finds, and we tell it whether it's accurate or not, it can continually find its own. But eventually we put in what we tell it to look through algorithm. AI obviously can take it to that next point where it can identify potential misuse on its own. That's my understanding, anyway.

CA Have you got any more details about the workings of the software you have a tender for, for the machine learning?

W No, so we've only got the requirements at the moment, what we would like it to do and what we'd like it to be able to ingest and export. And then that goes off to a different area who look at options and costings. But the money has been put there from The Cyber Defence Project. This is obviously an area we want to invest in. And Victoria Police is investing a lot of money in additional IT facilities and we're going more mobile, and the ability to conduct checks is now with 10,000 police members 24/7. They've got a mobile device with them. So we see that that's more of an opportunity for them, so we're investing in the machine learning to try and increase our detections.

PO Queensland Police have a system they call QLiTE. Are you familiar where that?

W No, sir, I'm not.

PO It's mobile, like a little iPad tablet device.

W Yes.

PO They can access it remotely and do those checks that you're talking about. Probably something similar to what you're talking about at Vic Pol.

W Correct. Yes, correct, we're a bit behind them, I believe, them, but it's similar. Ours is called IRIS, which is a tablet or an iPhone personally issued to the frontline members which they have got the permission to take home 24/7. So they have that ability to access our information 24/7.

PO The Police Service here is currently swapping to, for their case management and database requirements Resolve. What system does the Vic Pol use, IT system?

W So at the moment we have Interpose, which is a software from a company Distillery, and that is, at the moment, for our case management. It is still in project, rolling out to BAU at the moment is an analytics capability of Neo, which is from the Sass company, Sass. And that is a secondary system which ingests the source systems information and has the ability to provide analytics over the top of information from a number of our systems. That and LEAP is a system we've had since 1994 which Victoria Police still use, which is our database that links into our Vic Roads data and our records.

PO Thank you.

CA In the process of decision making, whether or not it is a breach, once you get the exceptions and reports generated, are there areas of grey? Could you explain?

W Well, there is. So particularly in relation to access of information. Obviously not everyone can have an understanding of what that employee is entitled to see, what they're currently working on. So if we do get to that point where we can't provide an operational reason for that check, we may go directly to the management and make inquiries directly to save a full-scale investigation. Alternatively, depending on the sensitivity of it, we may just escalate a grey one because we can't find a legitimate business need.

CA And who attends those meetings and how are the outcomes recorded or reported?

W So we have a protective security assessment group meeting every week as part of the Security Incident Registry. It has our subject matter experts in IT, information security, physical security, personnel security, plus we have our agency security adviser who is a Superintendent in charge of our division. We also have the information security adviser. And we round table all security incidents that we record in the week that are assessed of moderate or above. And we also use that to discuss things that we can't land on a decision on the path that the reports needs to take.

CA And that's weekly?

W That's every Thursday.

CA Thank you. I don't have any further questions for Senior Sergeant BELL.

PO Thanks very much, Senior Sergeant, thanks for coming. It’s been very helpful. You're excused.

W Thank you.

END OF SESSION