MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

18 APR 2019

Alex Harris
fyi-request-9355-bbe27c62@requests.fyi.org.nz

Dear Alex Harris

On 9 January 2019, you emailed the Ministry requesting, under the Official Information Act 1982, information regarding training received by ZX Security.

Your questions are addressed in turn below:

- *Whether your agency has ever employed ZX Security Ltd, to provide training in social media or open source intelligence. For the avoidance of doubt, I am not interested in any work done by them on network security or penetration testing.*

The Ministry can confirm there has been one case where two staff attended a ZX Security session on Open Source Intelligence on 9 December 2014. This was a public course run by ZX Security which was for the wider comunity. When the two staff attended the course they identified that some of the tools and techniques being promoted would not be appropriate for the Ministry to use. ZX Security offered subsequent sessions in 2015 and 2016 which were not taken up by the Ministry.

- *If so, all information relating to, or provided by, ZX Security Ltd in relation to the above.*

Please find attached a copy of the Ministry's correspondence with ZX Security in which training was offerred to employees. The names of some individuals are withheld under section 9(2)(a) of the Official Information Act in order to protect the privacy of natural persons. The need to protect the privacy of these individuals outweighs any public interest in this information.

You will also note that the contact details of some individuals have been withheld under section 9(2)(k) of the Official Information Act in order to reduce the possibility of staff being exposed to phishing and other scams. This is because information released under the Official Information Act may end up in the public domain.

Please also find attached two documents provided by ZX Security containing material in relation to the course attended by Ministry staff. You will note that the names of some individuals are withheld under section 9(2)(a) of the Official Information Act in order to protect the privacy of natural persons. You may note that the Statement of Work references training material being developed for the Ministry. Apart from the attached Statement of Work no training material was produced for the Ministry.

National Office, Aurora Centre / 56 The Terrace (off Aurora Tce) / Wellington 6011
56 The Terrace, Aurora Tce / Wellington 6011 / New Zealand
Fax: +64 4 918 3100 / **www.msd.govt.nz**

The Statement of Work was provided to ask if the Ministry wanted to have a dedicated session with ZX which was declined. The Statement of Work was produced prior to the two staff attending the course and realising that the tools and techniques were not appropriate for Ministry purposes.

The principles and purposes of the Official Information Act 1982 under which you made your request are:

- to create greater openness and transparency about the plans, work and activities of the Government,
- to increase the ability of the public to participate in the making and administration of our laws and policies and
- to lead to greater accountability in the conduct of public affairs.

This Ministry fully supports those principles and purposes. The Ministry therefore intends to make the information contained in this letter and any attached documents available to the wider public shortly. The Ministry will do this by publishing this letter and attachments on the Ministry of Social Development's website. Your personal details will be deleted and the Ministry will not publish any information that would identify you as the person who requested the information.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with this response regarding training by ZX Security, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Yours sincerely

Stephen Crombie
Deputy Chief Executive, Corporate Solutions

Out of scope

[redacted]

From: s 9(2)(a)
Sent: Thursday, 6 November 2014 1:49 p.m.
To: s 9(2)(a)
Subject: RE: OSINT Training & Kiwicon

Yes please - I have just confirmed things from my end.
I will be attending and will bring s 9(2)(a) one of our analysts.

Cheers

s 9(2)(a)
Senior Analyst
Intelligence Unit
Ministry of Social Development

E-Mail: s 9(2)(k)
DDI:
D2D:
Mobile:

Level 2, Bowen State Building, Bowen Street
PO Box 1556, Wellington 6140

[SEEMAIL]

From: Simon Howard [mailto:s 9(2)(a)
Sent: Thursday, 6 November 2014 12:03 p.m.
To: s 9(2)(a)
Subject: RE: OSINT Training & Kiwicon

Hi s 9(2)(a)

I can invoice you separately for the training if you like. Would you like me to book you in for the 9th of December then?

Cheers,
Simon

From: s 9(2)(a) [mailto:s 9(2)(k)
Sent: November 2014 3:50 p.m.
To: 'Simon Howard'
Subject: RE: OSINT Training & Kiwicon

Thanks for that Simon – unfortunately Kiwicon will conflict with other training we have scheduled. It does look like it would have been really interesting .
OSINT looks like it could work though, but if we do register it will just be for two of us at your group session on December 9.
Will keep you posted on that. Seeing as the purchasing link won't open for us, is there an alternative (do you do this on invoice?)

Cheers

s 9(2)(a)
Senior Analyst
Intelligence Unit
Ministry of Social Development

E-Mail: s 9(2)(k)
DDI
D2D
Mobile

Level 2, Bowen State Building, Bowen Street
PO Box 1556, Wellington 6140

From: Simon Howard [mailto:s 9(2)(a)
Sent: Wednesday, 5 November 2014 7:46 a.m.
To: s 9(2)(a)
Sub RE: OSINT Training & Kiwicon

Hi s 9(2)(a)

Yes, the training is being held in Wellington at the Auldhouse Training Rooms:
Level 8, Lumley House,
11 Hunter Street
Wellington
Computers are provided in the training suite, along with tea/coffee and lunch.

I have attached a statement of work which should provide all the necessary details, let me know if you have any questions or if you would like to catch-up for a coffee to discuss further.

I don't have a PDF of the talks so far, here is a copy and paste from the website, we have around 20 more talks to announce.

Title	Eve, Mallory, Ocean's 11, and Jack Bauer: Adversaries Real and Imagined
Abstract	In a post-Snowden world, it seems everywhere you turn you are faced

	with nation-state hacking, global network adversaries, hardware interdiction, baseband exploits, firmware backdoors, network injection, cyborg aliens, and a plethora of other threats. Once the realm of the underground, the black market, and intelligence agencies, intrusion and implant capabilities are now sold at trade shows for dictator pocket change. This talk will discuss the nature of targeted and untargeted surveillance, exploitation and intelligence gathering contrasted with the dangers faced by high risk users. We'll examine the commercialization of offensive technologies and the targeting of journalists, human rights workers, and activists. Drawing on original research and first hand case studies, this talk will discuss attacks on real people by real adversaries while attempting to provide a useful framework to enable sane operational security planning.
Location	Thu 11 0915 @ The St James Theatre
Duration	45 mins
Name	Morgan Marquis-Boire
Origin	San Francisco, USA
Bio	Morgan Marquis-Boire is a researcher and raconteur. From the dark underground of Auckland's goth scene, he now acts as the director of security for First Look Media. He still wears mirrorshades after dark. He is also a senior researcher and technical advisor at a couple of places like the EFF that are way more important than Kiwicon. His research on surveillance, censorship, and the targeting of activists and journalists, often documented side by side with his massive physique, has been featured in numerous print and online publications. Although the founder of First Look Media, Glen Greenwald, was described by our head of state as being a henchman, Morgan is gracious enough to bring a certain taut pertness to his henchman's henchman's jumpsuit.

Title	Security the Etsy way: Effective security in a continuous deployment culture
Abstract	Effective security teams know that understanding people is just as important as understanding technology, and that to achieve security of an organisation requires that the security function is constructive in problem solving and not to just block innovation. Much has been spoken about Etsy's engineering culture, and how continuous deployment and 'devops' have been embraced and developed, but how does security operate in such an environment? This talk will discuss the progressive tools, techniques and approaches the Etsy security team follows to provide security while not destroying the freedoms of the engineering culture that we all love so much. Topics will cover the building of an effective security organisation that is people rather than technology centric, and one that positions

	security to facilitate problem solving with fellow engineers rather than blocking progress through the fear of changing risk. The end result being a more honest and inclusive security approach, as opposed to the more common situation of a perception of security that becomes increasingly divergent from reality as engineers work to circumvent the imposed security constraints. Discussions and demonstrations of some of the novel tooling developed and released as open source by Etsy will also be discussed time permitting.
Location	Thu 11 1345 @ The St James Theatre
Duration	45 mins
Name	Rich Smith
Origin	New York, USA
Bio	Rich is the Director of Security at Etsy where he leads the fearless band of cyber-guardians that defend Etsy's members, sellers and knitted good from the evils of the Interwebs - Cross-site-stitching and sequin-injection are all taken in stride daily. Before Etsy Rich spent the previous 10 years focussed offensive R&D and consulting and holding positions at a variety of companies including Immunity Inc., Kyrus Technology and HP Labs culminating in the co-founding of a research focussed consultancy called Syndis in Iceland. In his spare time Rich like beer, noisy music and Python.

Title	Building a hipster catapult, or how2own your skateboard
Abstract	s 9(2)(a) and Richo do hilarious and nasty things to a skateboard. Bask in their revelry as they prove that paying several thousand dollars for a Bluetooth-controlled mechanical spear you stand on is actually a poor choice. There'll be banter about bluetooth, the release of some internal tooling to make this work possible, a couple of live demos probably culminating in some poor bastard getting hurt
Location	Thu 11 1715 @ The St James Theatre
Duration	30 mins
Name	Richo & s 9(2)(a)
Origin	San Francisco, USA
Bio	richo is a flat duck enthusiast from Melbourne, who hangs out in SF with the cool kids most of the time. mike ryan is a computer jerk from california who actually does this crap for a living. seriously **2 grand** for a wireless skateboard?!

Title	Eradicating the Human Problem
Abstract	People are a problem. We are tangled balls of emotional detritus that masquerades as a trusted member of society. Underneath this lacquered veneer of respectability however writhes a tiny pink squishy ball of vulnerability - the root of all evil, well the root of security issues anyway. Let me tell you a story, let me bend your brain and make you feel uncomfortable. I want to show you why we are all our own worst enemies, why we should never ever be trusted and why security people are the worst of them all. Then, I will cross the creepy line and introduce AVA, the first prototype automated human vulnerability scanner. A tool for automatically mapping networks of people, attacking them and measuring the results. A tool for spotting the weak link in an organisation. A tool to help remove the squishy human element of human security. This is the future, a first step towards a greater good or a dystopian nightmare. You're welcome.
Location	Fri 12 1130 @ The St James Theatre
Duration	45 mins
Name	Laura "ladynerd" Bell
Origin	Auckland, NZ
Bio	Laura is a reformed software developer, penetration tester, amateur python juggler and repeat meddler. She talks a lot and has been known to have opinions. She is the founder and lead consultant at SafeStack.io, a specialist agile information security company and lives in Auckland with her husband and daughter.

Title	Cyberwar before there was Cyber: Hacking WWII Electronic Bomb Fuses
Abstract	While the Allies went to war with mechanical and chemical bomb fuses whose origins dated back to the 19th century, Germany put a large amount of effort in the 1920s and 1930s into designing and fielding high-tech electronic fuses, which were far more reliable and versatile than standard chemical and mechanical ones. This led to an ongoing arms race that lasted throughout most of the war, with Allied bomb disposers coming up with increasingly ingenious ways of hacking the fuses and German armourers countering with ever-more- fiendish fuse designs. This talk covers the details of the contest between the attackers and defenders, and time and OSH regulations permitting will conclude with a demo of defusing a live 2000kg bomb[*]. [*] No it won't.
Location	Fri 12 1215 @ The St James Theatre

Duration	30 mins
Name	Peter Gutmann
Origin	Auckland, NZ
Bio	Peter Gutmann is a researcher in the Department of Computer Science at the University of Auckland working on design and analysis of cryptographic security architectures and security usability. He helped write the popular PGP encryption package, has authored a number of papers and RFC's on security and encryption, and is the author of the open source cryptlib security toolkit, "Cryptographic Security Architecture: Design and Verification" (Springer, 2003), and an upcoming book on security engineering. In his spare time he pokes holes in whatever security systems and mechanisms catch his attention and grumbles about the lack of consideration of human factors in designing security systems.

Title	Random() Adventures in Minecrosoftcraft
Abstract	2.5 billion dollars is a fair bit of money to spend on a game. It took about $1B for Elon Musk to launch a private space program including designing their own rocket engines from scratch, so it should go a fair way. Minecraft was obviously worth every cent. I will speak today about exploiting random number weaknesses to gain sweet server secrets from this fantabulous fantasy engine, and will be giving out code release treats. Let me know if you work out how to make a few billion from them.
Location	Fri 12 1600 @ The St James Theatre
Duration	15 mins
Name	Pruby
Origin	Wellington, NZ
Bio	Tim/pruby/whatever is not going to pretend to be a badass. If you undercharge him, he will hunt you down and PAY YOU BACK. He didn't have to bribe anyone to get in to the con this year, they let him in all legitimate like.

Cheers,
Simon

From: s 9(2)(a) [mailto:s 9(2)(k)
Sent: Tuesday, 4 November 2014 2:08 p.m.
To: s 9(2)(a)
Subject: FW: OSINT Training & Kiwicon

Hi Simon

I see OSINT is being held on 9 December. I presume this is in Wellington? We are looking at sending two people – myself and another analyst. The multi-agency group will be fine for us at this stage, but if you'd like to let us know what an MSD group booking might entail, we could consider that instead. There are 7 of us that could potentially attend something like this.

Also you mentioned in your email that OSINT was being held prior to Kiwicon, when and where is that taking place? And are you able to send me a PDF version of the speakers list?

Cheers

s 9(2)(a)
Senior Analyst
Intelligence Unit
Ministry of Social Development

E-Mail s 9(2)(k)
DDI
D2D
Mobile

Level 2, Bowen State Building, Bowen Street
PO Box 1556, Wellington 6140

From: Simon Howard [mailto: s 9(2)(a)
Sent: Monday, 3 November 2014 2:02 p.m.
To: s 9(2)(a)
Subject: RE: OSINT Training & Kiwicon

Hi s 9(2)(a)

As discussed attached is an overview of the course which I can run separately for MSD if you have enough interest. The agenda is customisable so if you want something specifically covered I am happy to accommodate.

The agenda for the Kiwicon sessions is slightly different and is as follows:

- Operational Security (OPSEC)
  - An overview of operational security processes and measures
  - Details of the various methods that can be used to mask your IP address and true identity
- Evidence Collection
  - An outline of the processes used to collect evidence for court proceedings
  - Tools, techniques and considerations for the collection of evidence
- Open Source Intelligence Gathering
  - Details of the open-source and social media sources that can be used to investigate an individual
  - A run through the tools (open-source and commercial) used for information gathering and analysis
- Emerging Social Networks
  - Analysis and overview of new social networks
  - Tools for connecting to social networks that are typically only available on mobile phones using your computer
  - Techniques to collect information from emulated environments
- Automated Harvesting of Content
  - Techniques for harvesting information from social networks and other sources with minimal programming knowledge
  - Issues to watch out for when automating information harvesting and solutions to these problems.
- Maintaining Multiple Covert Identities
  - Techniques used to identify a fake profile
  - How to maintain multiple identities across various social networks

- Techniques for creating a backstop for your online persona

Let me know if you have any questions.

Cheers,
Simon

From: s 9(2)(a) [mailto: s 9(2)(k)
Sent: Monday, 3 November 2014 11:42 a.m.
To: s 9(2)(a)
Subject: FW: OSINT Training & Kiwicon

Hi Simon

I'd be really interested in more info about both your OSINT training and Kiwicon. but can't get any of the links to work
Are you aware of anyone else having the same problem or is it just me?

Cheers

s 9(2)(a)

Senior Analyst
Intelligence Unit
Ministry of Social Development

E-Mail s 9(2)(k)
DDI
D2D
Mobile

Level 2, Bowen State Building, Bowen Street
PO Box 1556, Wellington 6140

From: s 9(2)(a)
Sent: Monday, 3 November 2014 8:43 a.m.
To: s 9(2)(a)
Subject: FW: OSINT Training & Kiwicon

FYI

s 9(2)(a) | National Manager
Intelligence Unit and Integrity Intervention Unit,
Ministry of Social Development
t: s 9(2)(k)
e:

From: s 9(2)(a) [mailto: s 9(2)(k)
Sent: Monday, 3 November 2014 8:40 a.m.
To: s 9(2)(a)
s 9(2)(a) s 9(2)(k) s 9(2)(a)
s 9(2)(a) (s 9(2)(k) s 9(2)(a)
s 9(2)(a)
s 9(2)(a) (s 9(2)(k) ; s 9(2)(a)
s 9(2)(a) s 9(2)(k)
s 9(2)(a)
s 9(2)(k) s 9(2)(a) s 9(2)(k) s 9(2)(a) (s 9(2)(k)
s 9(2)(a)
s 9(2)(k) ; s 9(2)(a)
s 9(2)(k) s 9(2)(a) s 9(2)(k) s 9(2)(a)
s 9(2)(a)
s 9(2)(a) s 9(2)(k) ; s 9(2)(a)
Subject: FW: OSINT Training & Kiwicon

Hi – please see the below from Simon Howard.

Regards,
s 9(2)(a)

s 9(2)(a)

CLAG

From: Simon Howard [mailto s 9(2)(a)
Sent: Sunday, 2 November 2014 19:12
To: s 9(2)(a)
Subject: OSINT Training & Kiwicon

Hi s 9(2)(a)

Just a quick heads up for the CLAG/ECLAG group that I will be running an Advanced OSINT Training session on Tuesday 9th of December prior my security conference – Kiwicon, It is open to anyone to attend.
There are still a number of places available at $800/head , people can buy the tickets online here: https://www.kiwicon.org/the-con/training/osint-training/ - Room hire charges will be covered by my company and all attendees will receive lunch.

Tickets for Kiwicon are also available here https://www.kiwicon.org/shop/product/kiwicon-ticket/ for the bargain basement price of $80/head for two days of in-depth information security talks. We have already sold 500+ tickets so best to get in quick.
We have announced the first round of speakers here to give those interested a taste of what is to come: https://www.kiwicon.org/the-con/talks/

Let me know if anyone has any questions.

Cheers,
Simon

--
Simon Howard
Security Consultant - ZX Security Limited

Phone: s 9(2)(a) | Email: s 9(2)(a) Web: www.zxsecurity.co.nz

---------- This email and any attachments may contain information that is confidential and subject to legal privilege. If you are not the intended recipient, any use, dissemination, distribution or duplication of this email and attachments is prohibited. If you have received this email in error please notify the author immediately and erase all copies of the email and attachments. The Ministry of Social Development accepts no responsibility for changes made to this message or attachments after transmission from the Ministry.

Simon Howard
s 9(2)(a)

Advanced Open Source Intelligence Training

ABSTRACT

The ZX Security Advanced Open Source Intelligence (OSINT) Training course is delivered as a day-long workshop in which we cover the techniques and tools used to conduct successful investigations on the Internet. By the end of the course, attendees will be able to produce relevant, timely and actionable intelligence.

COURSE OUTLINE

The course will be run as a series of modules with each module discussing one or more topics. Each topic will include hands-on exercises involving the course attendees where they will gain real-world experience with the tools and techniques discussed. The outline of the course is as follows:

Operational Security (OPSEC)- Introduction

- An overview of operational security processes and measures

Internet Fundamentals

- An overview of the building blocks of the Internet including IP Addressing, DNS and SMTP

Operational Security (OPSEC) – Remaining Undetected

- Details of the various methods that can be used to mask your IP address and true identity

Evidence Collection

- An outline of the processes used to collect evidence for court proceedings
- Tools, techniques and considerations for the collection of evidence

Open Source Intelligence Gathering

- Details of the open-source and social media sources that can be used to investigate an individual
- Use search engines effectively to find exactly what you are looking for
- A run through the tools (open-source and commercial) used for information gathering and analysis
- Details on how to extract meta-data from images including GPS details and device information
- How to connect to and monitor chat rooms and forums (both on the Internet and the Deep Web)

Maintaining Multiple Covert Identities

- Techniques used to identify a fake profile
- How to maintain multiple identities across various social networks
- Techniques for creating a backstop (history) for your online personas
- Systems and processes for sending and receiving anonymous messages

Workshop

- During this workshop the attendees will use the skills gained throughout the course to create a detailed dossier on a particular individual

LEARNING OBJECTIVES

- Increase the knowledge of attendees regarding Open-Source Intelligence (OSINT) Gathering
- Introduce attendees to the latest tools and techniques used to extract data from OSINT sources to support their day-to-day work activities

PREREQUISITE KNOWLEDGE

A basic knowledge of computers and the Internet is all that is required

WHO SHOULD ATTEND?

- Law Enforcement Personnel
- Corporate Security Professionals
- Fraud Investigators
- Auditors and Analysts
- Recruiters
- Background Check Professionals

REQUIREMENTS

- A Laptop capable of running VMWare Player
- Facilities in which ZX Security can deliver the course material which include a Projector

ZX Security can provide training room facilities and computers if required

SECURITY

MINISTRY OF
SOCIAL DEVELOPMENT
Te Manatū Whakahiato Ora

05/11/2014

Open Source Intelligence Training

Statement of Work

Version: 1.0

Table of Contents

1 Document Control

1.1 Document Information

Customer	MSD
Title	Open Source Intelligence Training - Statement of Work
Document Filename	MSD - OSINT Training SoW v1.0

1.2 Revision Control

Version	Date Released	Pages Affected	Author	Description
0.1	05/11/2014	All	Simon Howard	Initial draft

1.3 Distribution List

Name	Organisation	Title
s 9(2)(a)	Ministry of Social Development	Senior Analyst
Simon Howard	ZX Security Limited	Security Consultant

2 Background

Simon Howard met with representatives from the MSD to discuss the delivery of training material to MSD staff.

In order to assist MSD staff in performing their duties more efficiently, MSD has requested that training material be developed to cover tools and techniques used for gathering information from open-source and social media sources.

This statement of work details the tasks that will be conducted as part of the Open Source Intelligence (OSINT) training, the associated costs and estimated timeframes.

3 Objectives

The objective of this engagement is to:

- Increase the knowledge of the MSD investigation team regarding Open-Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT)
- Introduce team members to the latest tools and techniques used to extract data from OSINT/SOCMINT sources to support their day-to-day work activities

4 Scope

The scope of this engagement is as follows:

- Delivery of one full-day OSINT course to MSD employees

5 Approach

The approach used to deliver this presentation will be as follows:

- Research topics and prepare slide deck material
- Prepare workshop material including software and module tasks
- Deliver course material to MSD employees

6 Deliverables

The following deliverable will be produced as part of this statement of work

- One full-day course on open-source intelligence gathering techniques delivered as a PowerPoint presentation
- The course will run from 09:00-17:00 (8 hours)

The course will be run as a series of modules with each module discussing one or more topics. Each topic will involve hands-on exercises involving the course attendees where they will gain real-world experience with the tools and techniques discussed.

Module	Topic	Description	Duration (mins)
Operational Security - Introduction			
	OPSEC practices	An overview of operational security processes and measures	20
Internet Fundamentals			
	Internet fundamentals (DNS, SMTP, TCP/IP)	An overview of the building blocks of the Internet, description of how IP Addresses, DNS and SMTP work at a basic level	45
Operational Security – Remaining Undetected			
	Methods for masking your IP address	Details of the various methods that can be used to mask your IP address including TOR, VPNs' and Jump-hosts	30
	Virtualisation as a tool to avoid being compromised	Walk through the virtual machine environment which will be provided to each attendee and explanation of how the technology works	20
Open Source Intelligence Gathering			
	OSINT/SOCMINT information sources	Details of the open-source and social media sources that can be used to build a profile on an individual	25
	Using search engines like a pro	Using search engines to find exactly what you are looking for by becoming a google power user	20
	Tools and techniques used for information gathering	A run through the tools (open-source and commercial) used for information gathering and analysis	80
	Image metadata analysis	Details on how to extract meta-data from images including GPS coordinates and device information (e.g. mobile phone/camera model)	30
	Monitoring chat channels and forums	How to connect to and monitor chat rooms and forums (both on the Internet and the Deep	80

		Web)	
Procedures for evidence collection			
	Methodology	Details on the ACPO guidelines for the collection and storage of evidence	10
	Evidence Collection Tools	Tools used to collect and store data from online sources	10
Maintaining multiple covert identities			
	Detecting fake profiles	Techniques used to identify a fake profile. .	10
	Cross-posting & profile management	How to maintain multiple identities across various social networks	20
	Profile backstopping	Techniques for creating a backstop (history) for your online personas	20
	Anonymous cell phone numbers and email addresses	Systems and processes for sending and receiving anonymous messages (SMS and Email).	20
	Payment methods for purchasing services	How to pay for various services while maintain anonymity	10
Workshop			
	Creating a Dossier	During this workshop the attendees will use the skills gained during the course to create a detailed dossier on a particular individual	30

7 Project Structure

This project will be resourced as follows:

Role	Name	Organisation
Security Consultant	Simon Howard	ZX Security Limited

8 Assumptions

The following assumptions have been made:

- ZX Security will provide a location to hold the training course which has the necessary seating to accommodate the numbers and a projector to display the training material
- ZX Security will provide each course attendee with a computer to run the workshops on
- The course will be delivered to MSD staff in Wellington
- All work will be conducted during normal business hours

9 Project Schedule

Based on the scope of work as outlined above we have scheduled one session to be delivered on the following date:

- TBD

10 Project Costs

This assignment has been priced at a fixed-price for delivery of the course material and rental charges for the training room.

The itemised costs are as follows:

Item	Rate
Course Material Delivery (per person)	$800
Training Room Hire (1 day)	$990

All quotes exclude GST and disbursements. Should the project scope change, we will work with MSD to ensure an appropriate resolution can be reached.

11 Acceptance

The project as defined within this document is deemed acceptable, and gives approval to proceed with the assignment as described.

s 9(2)(a) - MSD

Date