Establishing a Framework for the Performance of Cyber Intrusion Investigation and Response

INFORMATION SHEET FOR PARTICIPANTS

Hello

You are invited to take part in this research. Please read this information before deciding whether to take part. If you decide to participate, thank you. If you decide not to participate, thank you for considering this request.

Ko wai ahau / Who am I?

My name is Luke Pearson and I am a Doctoral student in the Faculty of Science and Engineering at Te Herenga Waka—Victoria University of Wellington. This research project is work towards my dissertation.

He aha te whāinga mō tēnei rangahau / What is the aim of the project?

There is no communicable framework for investigating and responding to cyber intrusions. The currently understood process to become a good incident responder is to work under good incident responders and inherit the "tribal knowledge" they offer.

For the purposes of this research, an intrusion is the interactive access to more than one computing system by an attacker, where the access to subsequent systems is dependent on the compromise of previous systems. For example, two different systems being compromised by the same phishing campaign would not meet this criteria, but the compromise of one system leading to lateral movement to a second system would.

This project intends to capture the processes by which experienced incident responders like yourself investigate and respond to cyber security intrusions. Your participation will support this research by sharing your experience to help inform this framework. This research has been approved by the Te Herenga Waka—Victoria University of Wellington Human Ethics Committee 2026/HE040062.

Ka pēhea tō āwhina mai / How can you help?

You have been invited to participate because you have experience in performing or leading intrusion investigation and response activities.

You are someone who has either participated in a minimum of five intrusion investigation and response engagements, OR led a minimum of three such engagements.

If you agree to take part, I will interview you via Victoria University of Wellington's Zoom instance. The interview is made up of two parts:

1. I will ask you questions about your general experiences, and how you spend your professional time outside of actively responding to incidents. This phase of the interview will take approximately 30 minutes.
2. We will work through a tabletop scenario of a compromised environment. This will be used to capture your thought process and methodologies for incident response in an environment that doesn't require you to share any details of specific incidents you've worked. This phase of the interview will take approximately 60 minutes.

I will video record the interview with software running locally on my computer with your permission and use this recording to create formal notes once the interview is complete. You can choose to not answer any question or stop the interview at any time, without giving a reason.

Ka ahatia ngā kōrero ka tukuna mai / What will happen to the information you give?

This research is confidential. This means that I, as the researcher, will be aware of your identity, but the research data will be combined. Your identity will not be revealed in any reports, presentations, or public documentation.

A snippet of the recording which captures your consent to participate in the interview will be taken from the broader recording and retained until August 1, 2031.

The remainder of the interview recording will be erased once a complete transcript has been produced and validated. These transcripts will not contain your name, but rather a placeholder unique to you (for example, Participant 313). This transcript is expected to be produced, and the recording of your interview with your specific answers deleted, within 10 days of the interview taking place.

Your name, email address, a link to the recording snippet containing your consent, and choice to receive research outputs will be retained until August 1, 2031. This dataset will NOT link your identity to your placeholder.

In the event your feedback is quoted in publication or presentation, quotes will be attributed to your placeholder. These will be used sufficiently sparingly that no attribution to you will be possible. However, you should be aware that in small projects your identity might be obvious to others in your community.

Only my supervisors and I will read the notes or transcript of the interview.
The interview transcripts, summaries and notes will be kept securely and destroyed on August 1, 2031.

During the interview, you will provide the researcher a passphrase that is unique to you. This passphrase will not be stored with your identifying information, but with your de-identified transcript. In the event you wish to withdraw from the research, you will email the researcher, provide your passphrase, and advise you wish to withdraw consent. At this time, all research materials associated with this passphrase

will be destroyed. This is the only method by which your consent may be withdrawn, as it is the only method by which you can be linked to your transcript – I will not keep a mapping of participants to passphrases, to protect your privacy. I highly recommend choosing a memorable passphrase, or storing it in a secure location.

He aha ngā hua o te rangahau / What will the project produce?

The information from this research will be used in my PhD dissertation and potentially both academic and industry publications and conferences.

If you like, as a thank you for participating in this research, complete copies of published research outputs can be sent to you via email once they are finalised. Additionally, once the interviews are complete, the entire set of scenario documentation can be provided to you to use in whatever manner you fancy, for example, internal training of your teams.

Ki te whakaae mai koe, he aha ō mōtika hei kaitautoko i tēnei rangahau / If you accept this invitation, what are your rights as a research participant?

You do not have to accept this invitation if you don't want to. If you do decide to participate, you have the right to:

- choose not to answer any question;
- ask for the recording to be turned off at any time during the interview;
- withdraw from the study before February 1, 2027;
- ask any questions about the study at any time;
- be able to read any reports of this research by emailing the researcher to request a copy.

Mehemea ngā pātai, he raruraru rānei, me whakapā ki a wai / If you have any questions or problems, who can you contact?

If you have any questions, either now or in the future, please feel free to contact my supervisor or myself:

Student:	**Supervisor:**
Name: Luke Pearson	Name: Ian Welch
University email address: pearsoluke1@myvuw.ac.nz	Role: Research Supervisor
	School: Computer Science and Engineering
	ian.welch@vuw.ac.nz

He kōrero whakamārama mō HEC / Human Ethics Committee information

If you have any concerns about the ethical conduct of the research you may raise this with the HEC Convenor, Te Herenga Waka—Victoria University of Wellington, by emailing human-ethics@vuw.ac.nz or phoning the University's Service Centre on 0800 04 04 04.

Establishing a Framework for the Performance of Cyber Intrusion Investigation and Response

CONSENT TO INTERVIEW

This consent form will be held for a minimum of five years.

Researcher: Luke Pearson, Faculty of Science and Engineering, Te Herenga Waka—Victoria University of Wellington.

- I have read the Information sheet, and the project has been explained to me. My questions have been answered to my satisfaction. I understand that I can ask further questions at any time.
- I agree to take part in a video recorded (with software running locally on the researcher's computer) interview compromised of semi-structured interview questions and a tabletop scenario.

I understand that:

- I may withdraw from this study at any point before February 1, 2027, and any information that I have provided will be destroyed.
- The identifiable information I have provided associated with my specific answers will be destroyed as soon as interview transcriptions have been created and validated.
- Any information I provide will be kept confidential to the researcher and the supervisor.
- The findings may be used for a PhD dissertation and/or academic publications and/or presented to industry conferences.
- The interview notes, transcriptions and recordings will be kept confidential to the researcher and the supervisor.
- My name will not be used in reports and utmost care will be taken not to disclose any information that would identify me.
- If I would like to receive a copy of research outputs, the tabletop scenario, or both, I must contact the researcher and provide my email address for receiving this material.

Note: Any questions, as well as your formal consent to the above, will be captured and recorded at the start of your interview.