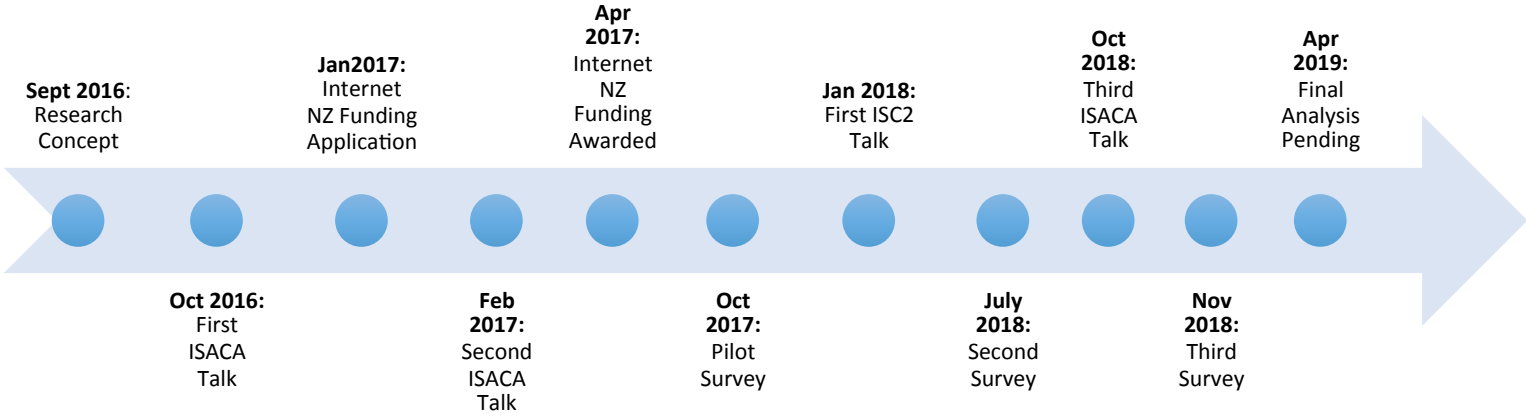
Final report template for Community Projects and Internet Research - to be sent to gertrud@internetnz.net.nz on the date specified in your contract	
Grant reference number:	#IR20160031
Name of recipient and contact details	*Chris Hails (chris@ubisec.nz / 021 506783)*
Name of organisation *(if applicable)*	
Title of project/research	A study to evaluate the programmatic identification of cyber security risk profiles that may in future facilitate the delivery of targeted or personalised risk mitigation interventions.
Amount of funding received	$9715
Budget details	*List a breakdown of any expenditure to date and compare it with your expected expenditure. Please account for any areas of overspend or underspend:* Research labour – 350 hours / $10,500 Surveying tools - $1080 Miscellaneous costs - $60 The project has taken significantly more time than originally planned due to the complexity of recruiting participants and the evolution of the original research hypotheses and surveying approach as initial data was evaluated. Expenditure beyond the original budget was focused on the online surveying tool, this was required for longer than originally budgeted and iterative survey tranches have required extended analysis after collection.

Project/research approach and methods	A comprehensive literature review was initially undertaken; analysis of existing research literature highlighted three widely utilised psychometric scales. A statement of ethics was drafted and reviewed and research outline published online. A pilot survey was developed and initial data analysis completed in accordance with the research hypotheses and according to the proposed project budget. The pilot survey requested basic respondent demographics and used the questions from the 3 selected psychometric scales to measure computer use, health and lifestyle factors and how they may shape risk appetite and risk perception. A second survey collected 167 responses through an anonymous web-based survey. The three scales are: • **SeBIS – Security Behavior Intentions Scale** Measures attitudes towards choosing passwords, device securement, staying up-to-date, and proactive awareness • **CFC – Consideration of Future Consequences Scale** Identifies individuals who are more inclined to act in ways that are protective of their future health and well-being (*only CFC-F future focused elements were used*) • **DOSPERT – Domain-Specific Risk Taking Scale** Assesses individual risk taking and risk attitude (*only recreational elements of DOSPERT–R were used*) Analysis of the data from the adapted second survey revealed promising findings and indicated that the approach should be statistically evaluated in greater detail. A further 700 participants have now taken part through a third survey but 300 more responses are still being sought to ensure the total sampling is representative of the wider NZ population as a whole. The research project is still ongoing and once the desired response level has been met this should enable final reporting and presentation of the overall outcomes.
Summary of project/research outcomes	**Second stage preliminary findings utilised both psychometric scales and demographic survey response data:** • SeBIS, CFC-F and DOSPERT-R scales used to identify 11 *Very High Risk* individuals from 103 validated responses • 36% of those identified had previously suffered a financial loss due to cybercrime; all bar one had experienced a security incident • More than half did not exercise and the remainder did significantly less than the study average (2hrs 5 mins)

	• Individuals who had suffered the highest number of incidents were more likely to smoke, take less exercise and not be saving towards their future. • They were also significantly younger than the survey median age at 33.8 (*Millennials*) • 55% of smokers and 42% of those who did not invest in their future had suffered a financial loss, compared with a survey average of 21% • 50% of those unemployed and looking for work had been a victim of cybercrime and had suffered a financial loss **Data analysis identified two groups of note – 22 'Victors' and 20 'Victims' based on self-reported answers to the second survey:** **'Victors'** Those who reported suffering no incidents or losses were older, predominantly female, less likely to smoke, keen investors, avid exercisers. 4% better at online safety and security practices (SeBIS) than the study average; slightly more future focused (CFC-F); 9% lower risk appetite than study average (DOSPERT-R). **'Victims'** Those who had lost money were more likely to be smokers, not actively investing, risk takers by nature. Less confident at online safety and security practices than the study average, scoring 10% below the Victors (SeBIS). Risk appetite 16% higher than the Victors (DOSPERT-R). In summary, the first two scales offer good 'predictive' insights into security knowledge and ability and future focused behaviour - Very High Risk (VHR) people are 'correctly' identified *to some extent* as victims of cybercrime. For DOSPERT-R, there appears to be a sweet spot at the start of the High Risk band; VHR recreational risk takers identified by the DOSPERT-R scale appear to be resilient 'Victors'. Combining the three scale scores via weighting or other means is required to produce a final Security Quotient metric. Further statistical analysis will help validate these preliminary findings (potential linear / logistic / multinomial regression). The small sample size for the second stage survey is an issue to prove that the Security Quotient model is both valid and repeatable. A larger survey dataset is necessary to validate the concept and two large employers have now provided a further pool of responses to analyse. A larger dataset (1000+) could allow nationality to be assessed for evaluation of Hofstede cultural 'Individualism' also being a protective/risk factor. The original project schedule as submitted has been significantly extended due to work and family commitments that required several trips to the UK and prevented progress. The report as submitted serves to give an insight on current findings.

Achievements	The initial literature review has generated significant learnings around socio-technical attacks, cyber psychometrics and shaped the research hypothesis. An initial pilot survey was developed focusing on demographic factors, security capabilities, risk perception and risk appetite in the form of 62 questions. Analysis of the data generated suggests the Security Quotient scale may facilitate indicative identification of cybersecurity risk profiles. After presenting the initial findings at ISC2, this generated more interest in the project aims from CFFC, ConnectSmart (https://www.connectsmart.govt.nz/alertsnews/internet-security-researcher-seeks-assistance-from-cybercrime-victims/) and the wider media resulting in coverage of the research concept and second public survey in July 2018. As the summary data shows above, the model as hypothesised does appear to have some validity for identifying high-risk individuals who may be predisposed to being victims of cybercrime. Further analysis and research is required to confirm these preliminary findings.
Difficulties	The overall research project was slowed by existing work and family commitments and a serious unexpected illness affecting one overseas family member that required several visits to the UK. It proved difficult to engage with University of Auckland academics due to their existing commitments and overall lack of interest in the project due to the hybrid nature of the 'cyber psychology' approach. This was initially mitigated by seeking the assistance of academic contacts overseas and has resulted in new interest being sparked at AUT to take the statistical analysis and overall reporting to a conclusion later in 2019.
Findings/learnings	The project update *"AI scammers, holographic PMs and losing the race to the research pole - May 19, 2018"* included in the appendices discusses the work of researchers at the Universities of Cambridge and Helsinki to develop the 'Susceptibility to Persuasion II (StP-II)' test that can be used to predict who will be more likely to become a victim of cybercrime. The researchers had used the 12-item Consideration of Future Consequences Scale and confirmed that self-control is an important predictor of various behaviours including victimisation. The researcher only learnt of this UK-based work upon publication and the similarities in developing an early intervention model using pre-existing scales are interesting. Modic's StP-II scale drops to 54 core items to measure susceptibility to persuasion and the test is now available online. The literature review undertaken and iterative survey design process that forms the basis of this project has allowed the researcher to validate a data based approach to identifying cyber security risk profiles that may in future facilitate the delivery of targeted or personalised risk mitigation interventions. If the Security Quotient model can be fully validated through final analysis of the third

	stage survey responses and found to be repeatable there is the possibility that the approach could be used to target cybercrime prevention and intervention efforts to the subset of individuals at the greatest risk of victimisation. Learnings from other risk based modelling approaches can also be used in future work to benefit from research efforts developed predominantly for commercial underwriting gains in the US personal, life and auto insurance markets and known links to other behavioural risks such as financial lending. The advanced US lending and insurance markets have increasingly targeted indicative aspects of psychometric/behavioural relationships with claims histories and credit scores. Recent research has shown that both outcomes are influenced by sensation seeking/self control theories that match other OCEAN personality traits that can be measured using the CFC-F and DOSPERT-R scales. Psycho-social (personality) and biochemical (biological and inheritable trait) links have increasingly been shown to predict risk-taking behaviour in one realm also maps to risk-taking behaviour in others. In our increasingly data-rich environments, insurers in the US are looking to leverage such data to evolve the insurance marketplace as predictors of loss prospensity.
How have you shared your learnings from this project/research?	The initial hypotheses for the Security Quotient research project and iterative findings of the research approach have been presented over the course of the timeline shown below: 

	Project updates have been shared on the dedicated website at https://www.ubisec.nz and are included in the appendices to this report. The preliminary findings from the second survey included in the appendices were presented to the ISACA Cybersecurity Day in October 2018 which included members of the Auckland security and risk communities and a representative from CERT-NZ. Fraud experts from two major financial services companies expressed interest in the risk profiling concept and provided access to their staff; approximately 700 responses were received from the third survey and need to be completely analysed to assess alignment with the smaller second stage results.
Do you anticipate their being anything media-worthy in your project/research*	The initial findings in the appendices highlight the potential to use cyber psychology in the form of the Securiy Quotient scale to identify potential high risk individuals who may be more predisposed to fall victim to common socio technical attacks like phishing. Whilst this data has yet to be statistically validated by a larger sample the researcher would prefer the current findings are treated as preliminary.

Appendices

Research updates published online as the project progressed and project information as presented to external audiences is included:

- **Securing the human: a $35m question** - July 28, 2017

- **Cybersecurity research: guinea pigs wanted!** - September 27, 2017

- **AI scammers, holographic PMs and losing the race to the research pole** - May 19, 2018
  Discusses the work of researchers at the Universities of Cambridge and Helsinki to develop the 'Susceptibility to Persuasion II (StP-II)' test that can be used to predict who will be more likely to become a victim of cybercrime.

- **Press Release: Internet Security Researcher Seeks Assistance from Cybercrime Victims** - 26 July 2018

- **Securing the Human: The Science of Stupid? - ISACA Auckland Chapter Cyber Security Day** - October 18, 2018
  Presentation summary: **"**People are often considered the weakest link in the information security chain with human vulnerabilities able to be targeted by skilled attackers. My research project is focused on establishing if it is possible to accurately measure an individual's online 'Security Quotient' score – that is, the likelihood of falling victim to socio-technical cyber-attacks such as phishing emails, malware infection and internet scams based on analysis of Big Five personality traits. The ultimate aim: developing predictive analytics utilising psychometric profiling to prevent internet users from falling victim to cybercrime."

- **Securing the Human: The Science of Stupid?** - October 22, 2018

Securing the human: a $35m question

This post was originally published on LinkedIn on 28 July 2017

Chris Hails, Information Security Consultant
Browsing the BBC website this morning, a quote in a report on Alex Stamos' keynote to Black Hat jumped out at me. Facebook's CSO was talking about the need for 'a more people-centric security industry' and suggested:

"We have perfected the art of finding problems without fixing real world issues," he told attendees. "We focus too much on complexity, not harm."

The human side of information security and associated online harms is a major focus for me. Between August 2010 and August 2016, New Zealanders reported almost 28,500 online incidents to NetSafe involving $35m in direct financial losses.

In policing terminology there's a difference between pure 'advanced cybercrime' and cyber-enabled crime but when you've spoken with individual victims who have lost their life savings thanks to some shady overseas operator, the difference tends to melt away and the impact on the victim is what matters the most.

Think of the individual who has remortgaged their house; drained their business of operating capital; traveled to a hotel room thousands of miles away to meet that mysterious investor offering a handsome percentage in return for a small up front payment.

Those experiences at NetSafe left me wanting to find solutions to what are increasingly known as 'socio technical attacks'. If you haven't heard that term before I'll refer to Dr Jean-Louis Huynen: "A socio-technical attack is possible because of the human components in a system."

Over those six years working at NetSafe, the most common – and most financially and/or emotionally harmful – forms of socio-technical attacks were:

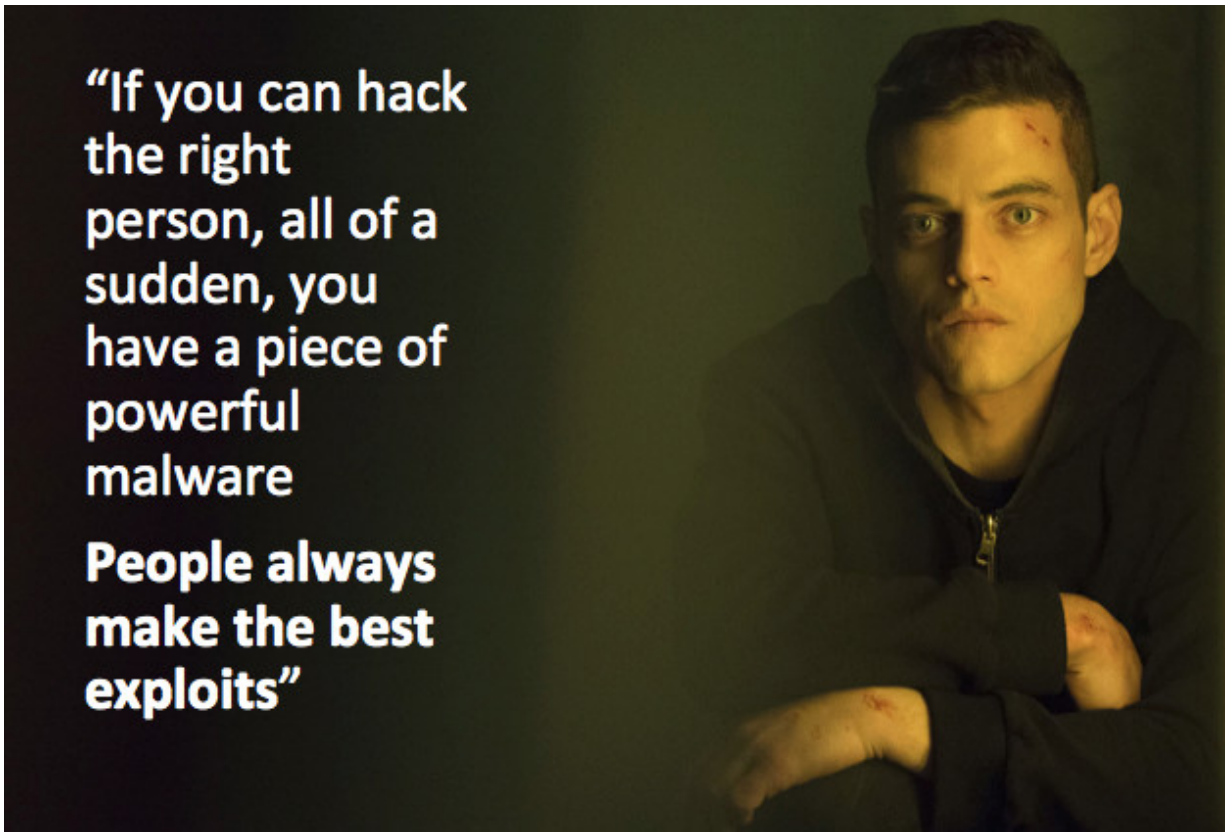
- Romance fraud
- Investment fraud
- Ransomware
- Business Email Compromise (BEC)

Whether you classify those as cyber-enabled or pure cyber attacks isn't the important point here. The key is that in the majority of those cases, the weakest link in the system was often a human being – a human who responded to the charms of a scammer or was curious enough to infect their own system and encrypt essential data.

Humans, it's fair to say, can be wonderful things but they also come with a range of inherent flaws or vulnerabilities:

- Many of us like to help people: that could be holding a door open for someone wearing a hi-vis vest piggybacking into a building or allowing the helpful 'Microsoft' technician to have access to your computer to fix the viruses.
- Many of us respond to outside forces or biases in the form of authority, curiosity or a general sense of invincibility and click on the malicious attachment or submit our credentials to the phishing site that 'satisfices' our need to verify it really is the official bank website.

These concepts are not new and whilst a smattering of the word cyber adds a sexy sheen to the stories, humans have been taken advantage of for a long time. Take a quick peek at this 'Spanish Prisoner' story in the New York Times and note the date: 20 March 1898.



What cyber brings to the picture is a speed of operation and ability to bridge the distance unimaginable for the criminals operating at the end of the 19th century. Speed and ease of operation and access to a global pool of victims equals profit and has resulted in changing the face of modern crime.

Look at the latest UK crime statistics and you'll find that 'cyber crime' in the form of Computer Misuse and Cyber Enabled Fraud now makes up 53% of reported crime.

There's no doubt that the technical skills involved in advanced, persistent, technically impressive attacks are to be reviewed with a wry smile and a sense of awe.

But it's becoming apparent that a failure to implement basic cyber hygiene steps – not sophisticated attackers – is often to blame. And that includes failing to train your staff on how to recognise suspicious activity and how to respond to potential cyber incidents.

Dr. Ian Levy, from the UK's National Cyber Security Centre probably said it best:

"A lot of the attacks that we see on the internet today are not purported by winged ninja cyber-monkeys. Attackers have to obey the laws of physics; they can't do things that are physically impossible"

The wonderful people at InternetNZ have provided me with funding this year to explore some of the root causes of those 28,500 incidents, to research why so many socio-technical attacks are successful and to examine if there might be a programmatic way to identify individual cyber security risk profiles and deliver adaptive security benefits in future.

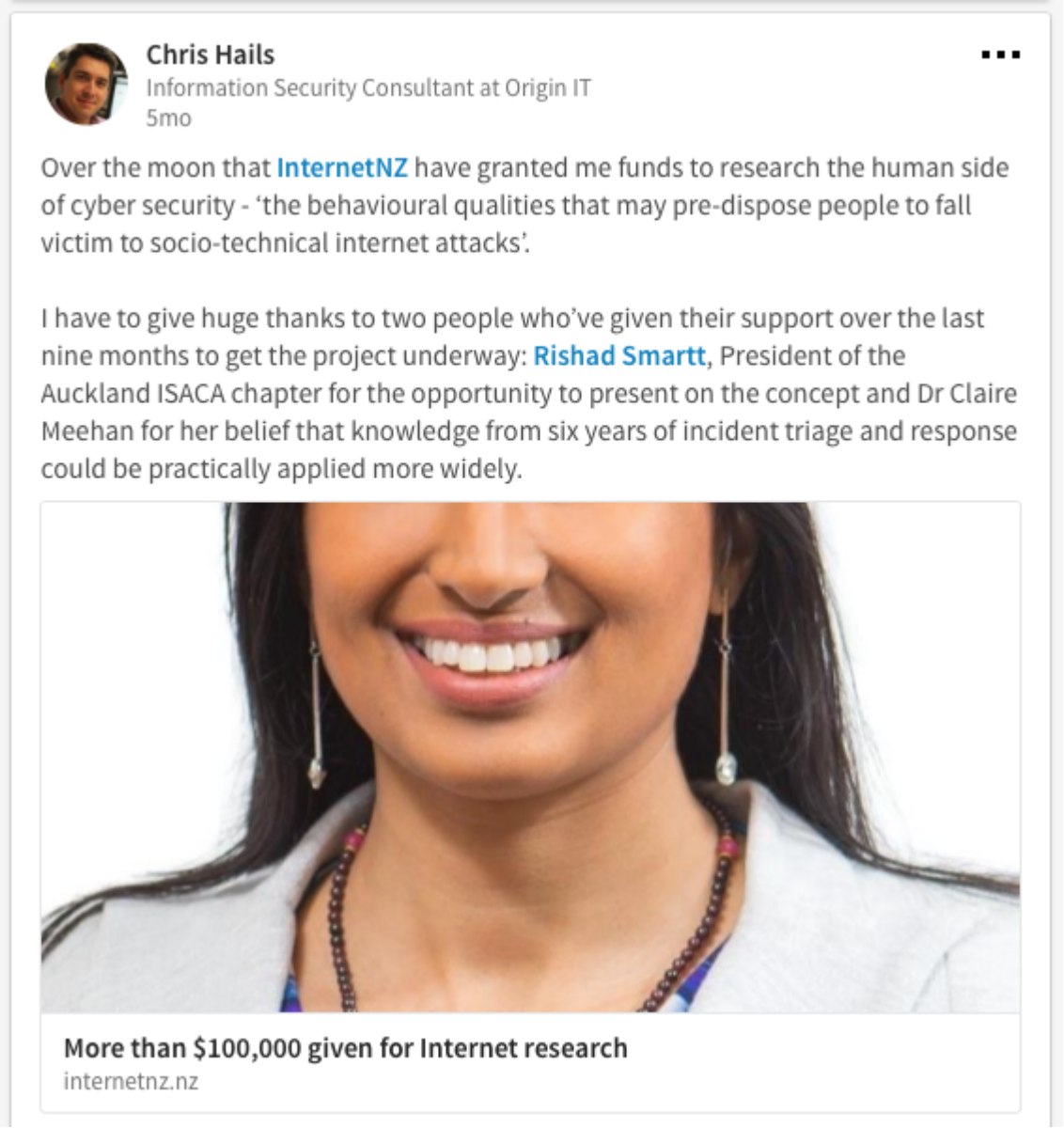
It's only the start of the project, but I'll be posting updates as I progress in the hope we can continue to explore ways to help more people stay safe and secure online.

Send me a message or leave a comment if you'd be keen to hear more.

July 28, 2017 ubisecusr socio-technical attacks

Cybersecurity research: guinea pigs wanted!

It's been a while since I celebrated getting funding from InternetNZ to research the human side of cyber security and how individual personality traits might play a part in common 'socio-technical attacks' like phishing, ransomware and online scams.



I've digested mounds of academic research spanning fields as diverse as human computer interaction, risk management, health promotion and social psychology. I've read books and blogs on social engineering and scammer tactics and have assembled the first draft of a conceptual scale that might help identify 'high risk' individuals when it comes to common cybercrime and cyber security attacks.

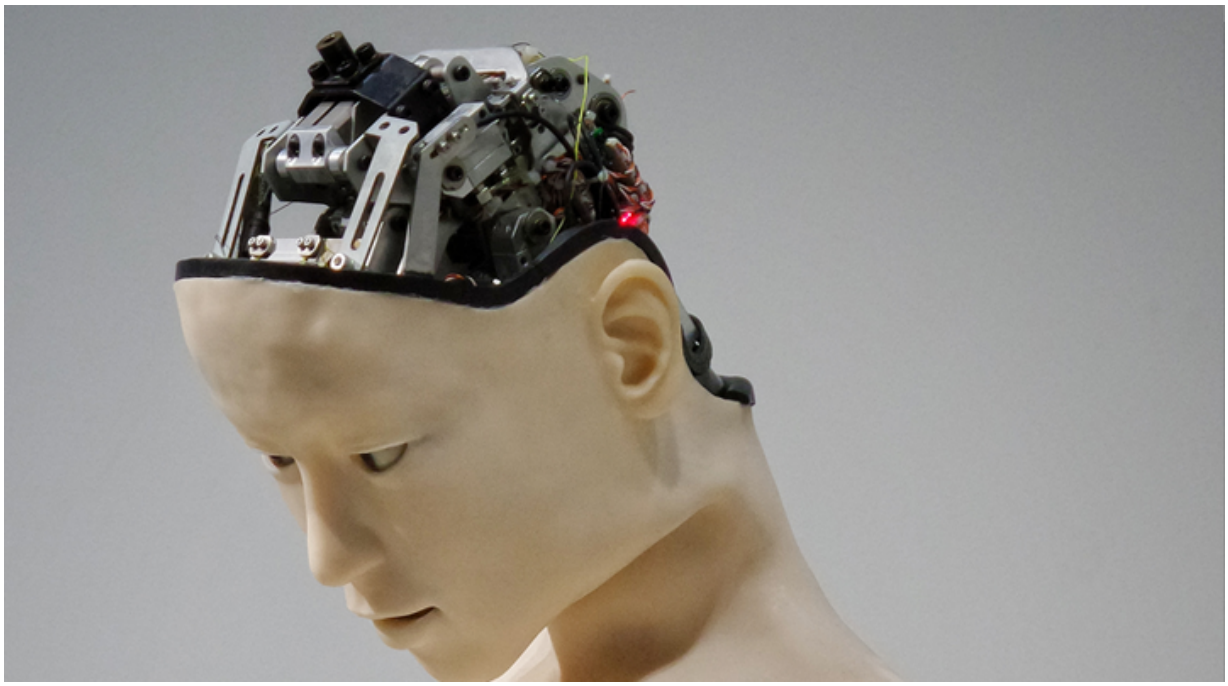
Taking inspiration from the agile "move fast and break things" mindset, it's highly likely this will be the first of many iterations of a research questionnaire but I'm keen to get feedback from some willing guinea pig volunteers.

If you have 15 minutes to spare and the enthusiasm to road test an online survey, please do get in touch by email to research@ubisec.nz or message me on LinkedIn and I'll happily share a URL with you.

The survey looks at basic demographic details, computer use, health and lifestyle factors and how they may shape risk appetite with the ultimate aim being to vulnerability scan layer eight.

Header image by David Burke, used under Creative Commons licence.

September 27, 2017 ubisecusr socio-technical attacks



AI scammers, holographic PMs and losing the race to the research pole

We live in interesting times.

If a royal wedding watched by half the planet or the pending implementation of an EU privacy regulation doesn't float your boat – *5 days to GDPR!* – tomorrow New Zealand's Prime Minister will address the crowds at Techweek in holographic form. Likely so she can keep up with work commitments and be in two places at once and who wouldn't benefit from cloning themselves to stay on top of email.

"Help me NZ techies, you're my only hope…."

Meanwhile the boffins at Google have taken decades of research into AI and computer speech synthesis and produced an autonomous assistant in the form of 'Duplex' that can book a hair appointment for you and sound uncannily real in the process. Parody makers start your engines…

If the loping, door-opening robots of Boston Dynamics doesn't have you reaching for that classic 80's Terminator DVD, Juha Saarinen's observations of Duplex's abilities in adversarial human hands should prove a lightbulb moment:

> *Humanity has an infallible ability to subvert and pervert the coolest technology, and use it to hurt each other with.*
>
> *Unfortunately, it's all too easy to imagine how Duplex could be misused by robocallers and phone fraudsters who won't start off the conversations with a "you are talking to an AI" warning.*
>
> *Think email spam, phishing, romance scamming and 419ing, except they'll arrive on your mobile phone.*
>
> *More naturally sounding and behaving digital assistants backed by self-learning AI will make them more attractive to people, not less, so expect to speak to machines more often.*

Google CEO Sundar Pichai told cheering crowds that Duplex understands the context and the nuance of conversation, a mean feat for those of us struggling to improve our EQ scores. The result of his Duplex demo was a concern that more effort should be made on protecting the human to prevent AI deception.

As someone researching human vulnerabilities and the role they play in socio-technical internet attacks, this latest development reminded me just how far behind in my project timeline I've slipped in 2018.

In January this year I presented an update on pilot survey data that looked promising based on research into OCEAN personality facets and the role they may play in social engineering susceptibility.

OCEAN PERSONALITY FACETS

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
+ Technological experience and computer proficiency - Tendency towards fantasy makes phishing lures appealing	+ More likely to follow training guidelines + Less likely to break security policies + Less likely to engage in insecure behaviours - Low levels predict deviant workplace behaviour such as breaking rules, or behaving irresponsibly	- High extraversion led to people giving up sensitive information because they wanted to gain acceptance or to belong to some social group (people that did not disclose their passwords were thought of as unsociable and not team players)	- Trust facet of this domain is targeted directly by phishers - Altruism facet of this domain is targeted directly by phishers - High levels associated with susceptibility - pursue communal goals and seek interpersonal harmony	+ Paranoia: may not share personal info + Computer anxiety: reduced technical experience / spend less time online / have fewer accounts + Good at identifying spearphishing - Impulsivity predicts poorer detection of phishing emails

The pilot survey requested basic demographics and used 62 questions from 3 psycho-metric scales to measure computer use, health and lifestyle factors and how they may shape risk appetite and risk perception:

SeBIS – Security Behavior Intentions Scale
Measures attitudes towards choosing passwords, device securement, staying up-to-date, and proactive awareness

DOSPERT – Domain-Specific Risk Taking Scale
Assesses individual risk taking and risk attitude

CFC – Consideration of Future Consequences Scale
Identifies individuals who are more inclined to act in ways that are protective of their future health and well-being

Five basic hypotheses underlie the research:

1. An average individual with average security knowledge, an average appreciation of future consequences and average propensity for risk taking scores 60% across all three scales.
2. Does security knowledge, an appreciation of future consequences and a risk averse nature result in higher scores?

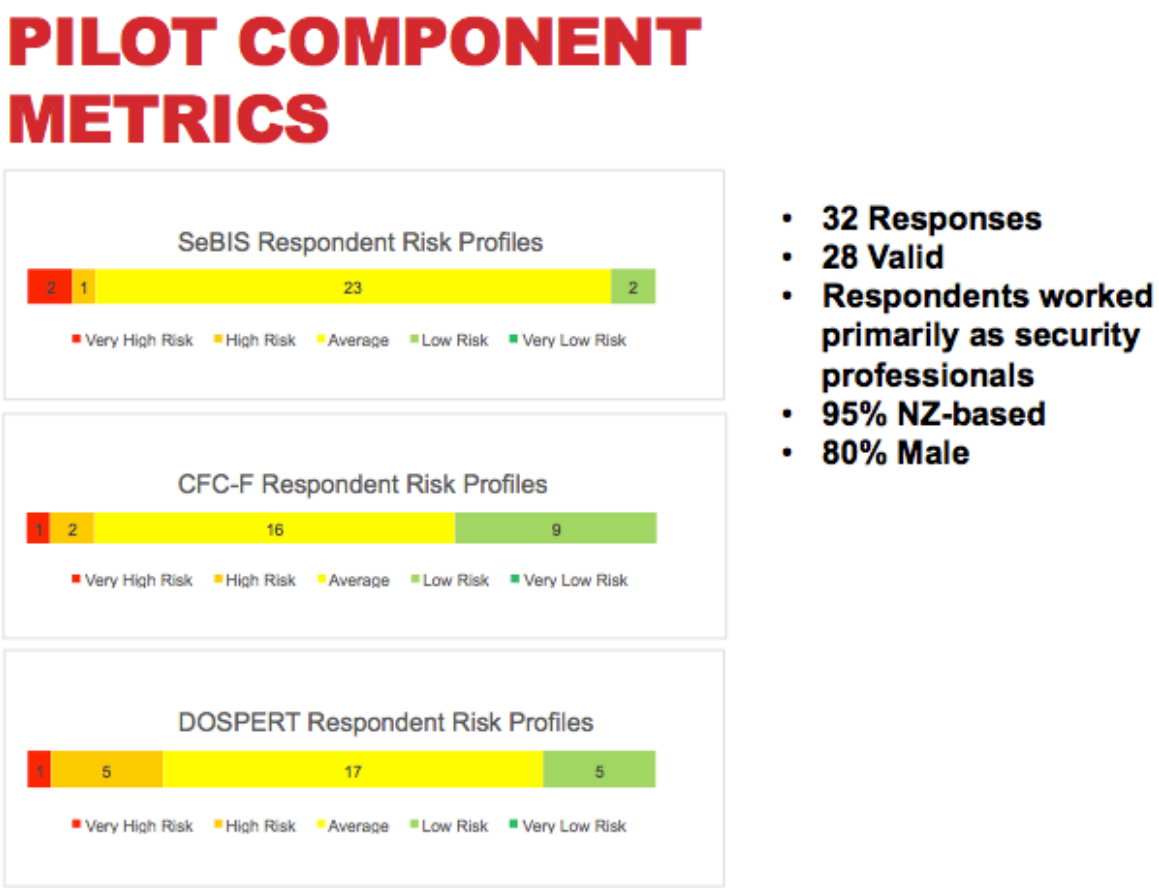
3. Does a lack of security knowledge, a desire for immediate returns and a risk taking or sensation seeking nature result in lower scores?
4. Does a lower score correlate with previous adverse experiences? Requires next stage data bearing evidence of cybercrime/security impacts, e.g. Falling victim to credential harvesting, financial losses.
5. Can we prove that a low score is predictive of being pre-disposed to socio-technical internet attacks?

The high-level concept being to generate a 'Security Quotient' score and to see if it's possible to test for high-risk human behaviour and mitigate it through additional security controls or by educating people in a targeted manner to mitigate those risks.

In short, can predictive analytics utilising psychometric profiling prevent internet users from falling victim to cybercrime.

Could personality profiling be used for more than just targeted advertising remarketing on search engines and social media? What if you could understand and quantify the nature of the people risk in your organisation as you can the technology risk?

Results from the pilot showed a distribution of scores from 28 valid responses with one anonymous respondent identified as very/high risk on two of the three scales:



To those attending, I summarised the next steps:

- A larger survey dataset is necessary to validate the 'average individual score' concept of 60%.
- Submissions by victims of cybercrime are required to validate the predictive ability of any such Security Quotient score.
- Nationality should be captured in the full survey for evaluation of cultural 'Individualism' being a protective factor

2018 project delays

A mix of family commitments and a new role working in Deloitte's cyber team has pushed back the final survey by three months. The race is now on to complete this second stage and write up the findings.

Race might be the wrong word though. Two weeks ago – thanks to a good friend working in Westpac's security team – I discovered that researchers at the Universities of Cambridge and Helsinki had developed the 'Susceptibility to Persuasion II (StP-II)' test that can be used to predict who will be more likely to become a victim of cybercrime.

Whilst this initially left me feeling like Robert Scott beaten to the South Pole by Roald Amundsen (*but without the cold and suffering*), my reading of their work suggests the Security Quotient concept is still valid.

Dr David Modic's team developed the StP-II scale with an initial 138 items based on significant research into scam compliance. They had used the 12-item Consideration of Future Consequences Scale and confirmed that self-control is an important predictor of various behaviours including victimisation. Lack of premeditation – thinking before you act – is a significant predictor of scam compliance. They also made use of the full DOSPERT-R scale (as opposed to just the recreational risk elements highlighted by Elie Bursztein's 2016 research into USB drops) to evaluate individual risk preferences.

Read the full research and you find the eventual StP-II scale drops to 54 core items to measure susceptibility to persuasion. The best part is the test is now online so give it a go and see how your personality stacks up.

But please be sure to take the updated Security Quotient survey once the final tweaks have been made, hopefully later this month, I don't want to suffer the fate of Antarctic explorers…

Photo by @franckinjapan

May 19, 2018 ubisecusr

Privacy Policy / 2018

Press Release: Internet Security Researcher Seeks Assistance from Cybercrime Victims

Date
26 July 2018

An Auckland researcher is seeking the assistance of 1000 New Zealand internet users as part of a project to understand the nature of human risk factors in the world of cyber security.

Chris Hails is a member of Deloitte's national cyber security team by day but spends his spare time on a research project funded by InternetNZ to assess an individual's 'Security Quotient' score.

By taking an online survey, Hails hopes to be able to identify internet users who may be more likely to fall for social engineering tricks such as email phishing and other common scams that rely on exploiting human vulnerabilities.

"My aim is to use psychometric profiling to prevent Kiwis from falling victim to cybercrime," said Hails who became passionate about finding a solution whilst working at NetSafe.

"Between August 2010 and August 2016, New Zealanders reported almost 28,500 online incidents involving $35m in direct financial losses," said Hails.

"Speaking with hundreds of victims who had lost anywhere from a couple of hundred dollars to more than $2m to ransomware, business email compromise, investment scams or romance scams made me realise there's a real need to identify high-risk human behaviours and mitigate it through additional security controls or by educating people in a targeted manner."

Hails went on to work at the National Cyber Security Centre, part of GCSB, where phishing attacks designed to harvest usernames and passwords or infect a computer remained the number one method of choice for advanced attackers targeting New Zealand organisations.

“Phishing is popular across cybercrime gangs and nation state actors simply because it works - computer users are vulnerable to deception, clicking on malicious links or opening attachments.”

A pilot Security Quotient survey requested basic demographic details and used 62 questions from 3 psychometric scales to measure computer use, health and lifestyle factors and individual risk appetite and risk perception.

“That initial data suggested that 3-4% of people may be more vulnerable to social engineering attacks based on facets of their personality,” said Hails.

The survey has now been improved upon and Hails needs 1000 New Zealanders to help progress his research. “Anyone over 18 is welcome to take the survey. If you’ve previously been a victim of cybercrime that would also help confirm if the scoring mechanism is effective and could help prevent people suffering harm in the future.”

More information on the study is available at https://ubisec.nz/ (https://ubisec.nz/). The Security Quotient survey is now available at https://www.surveymonkey.com/r/SecurityQuotient (https://www.surveymonkey.com/r/SecurityQuotient).

SECURITY QUOTIENT

Preliminary assessment of survey data

SURVEY - PROFILE

- 167 responses to the survey over 60 days
- 103 responses considered complete and valid
- 101 residing in NZ, 2 overseas, 18 different nationalities
- 52% Female, 48% Male reflective of the NZ population
- Survey median age was 46.1. Median NZ age is 36.9
- Underweight in BoP, Canterbury, Otago and Waikato
- Overweight in Wellington
- Overweight in the 35 – 54 year age band
- Survey respondents were heavily overweight in qualifications compared to the NZ population

SURVEY - LIFESTYLES

- **14% smoked vs. 16% across NZ (*MoH, 2017*)**
- **On average, exercised for 3 hours and 5 minutes per week**
- **80% actively saved or invested towards retirement**

SURVEY – CYBERCRIME

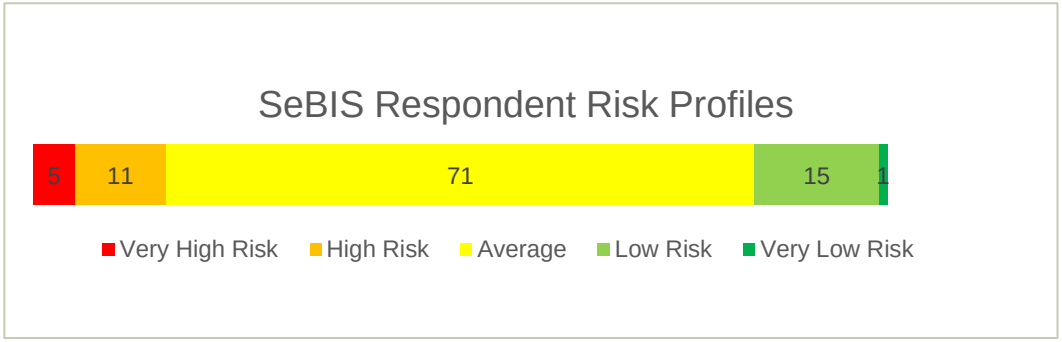
- **43% of respondents believed they had been a victim of cybercrime**
- **79% had suffered some form of cyber incident**
- **81 individuals had collectively suffered 142 incidents**
- **22 people had suffered a financial loss. Two had lost up to $10,000, one had lost up to $50,000. The average loss suffered was $2059**

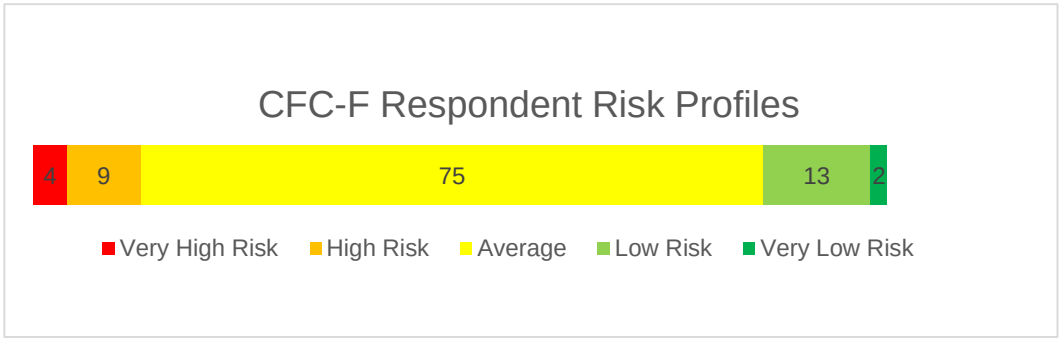
SURVEY – CYBERCRIME

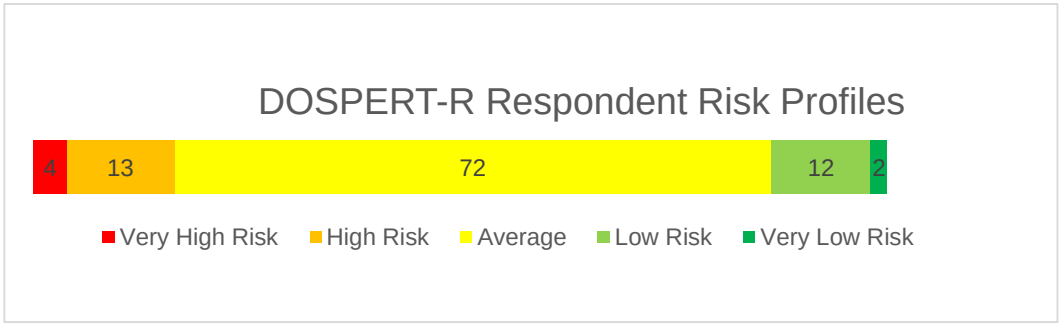
Have you been affected by one or more of these common forms of cybercrime?

Had a device infected by a virus or malware	46
Had an account password compromised	35
Had an email account or social media account hacked	22
Discovered fraudulent transactions on a credit card used online	19
Made a payment online that turned out to be a scam	7
Clicked on a phishing email and provided personal information	6
Experienced a device or data encrypted by ransomware	4
Had a website defaced or data compromised	3

PSYCHOMETRIC PROFILING

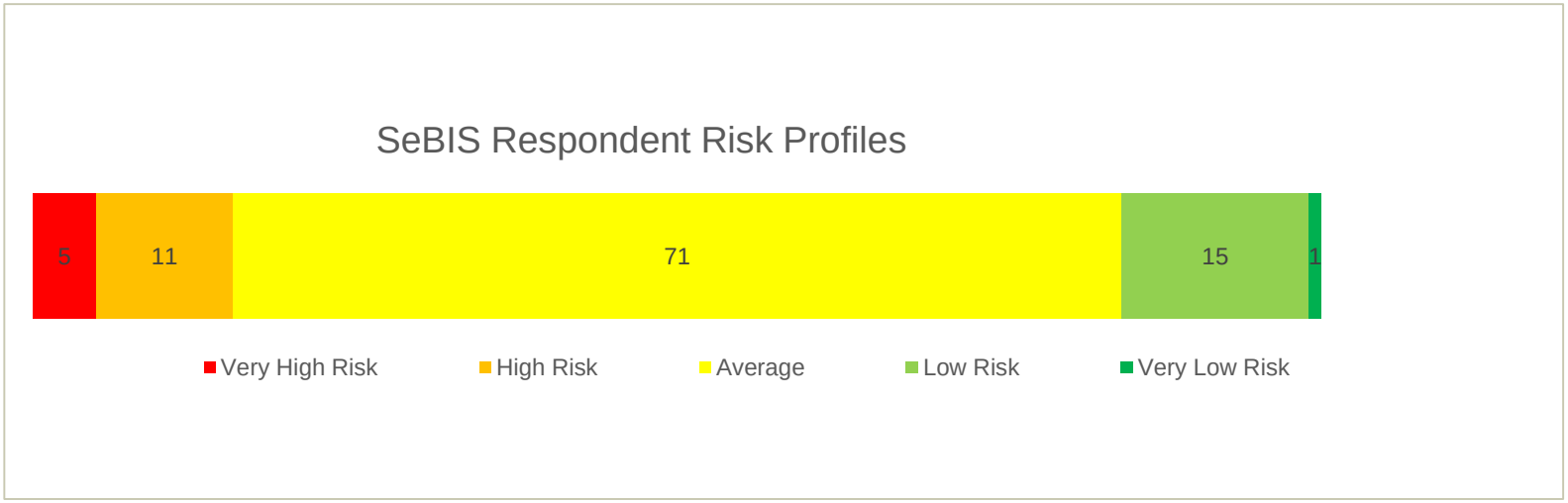






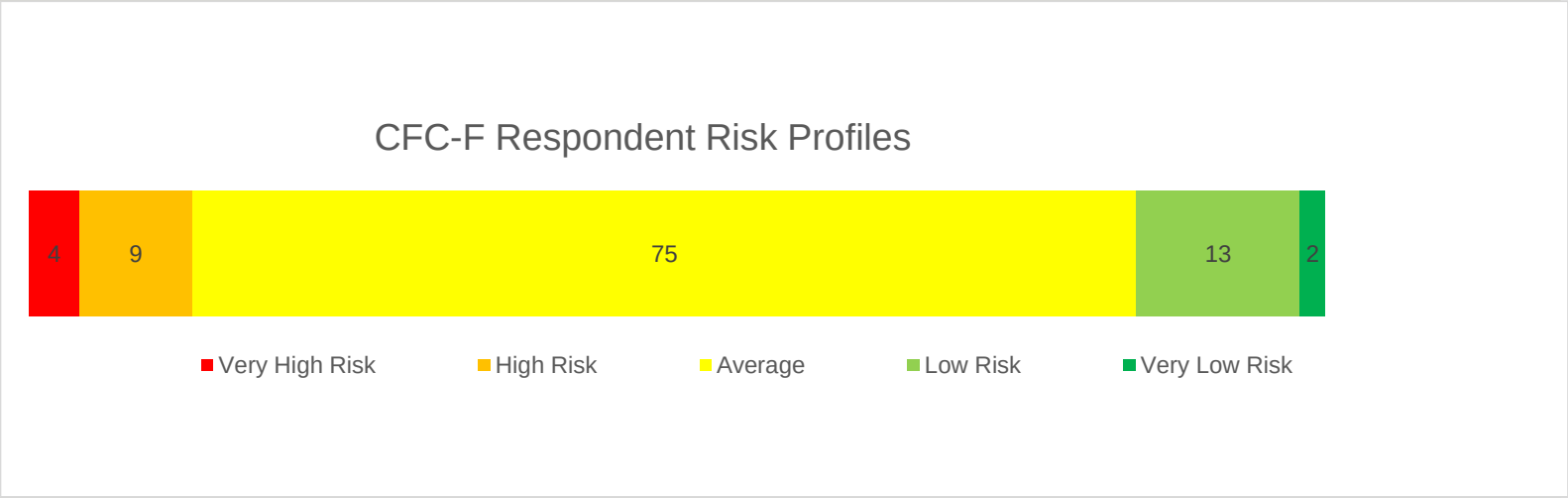
- **SeBIS, CFC-F and DOSPERT-R help identify 11 *Very High Risk* individuals**
- **36% of those identified had previously suffered a financial loss due to cybercrime; all bar one had experienced a security incident**
- **More than half did not exercise and the remainder did significantly less than the study average (2hrs 5 mins)**

PSYCHOMETRIC PROFILING



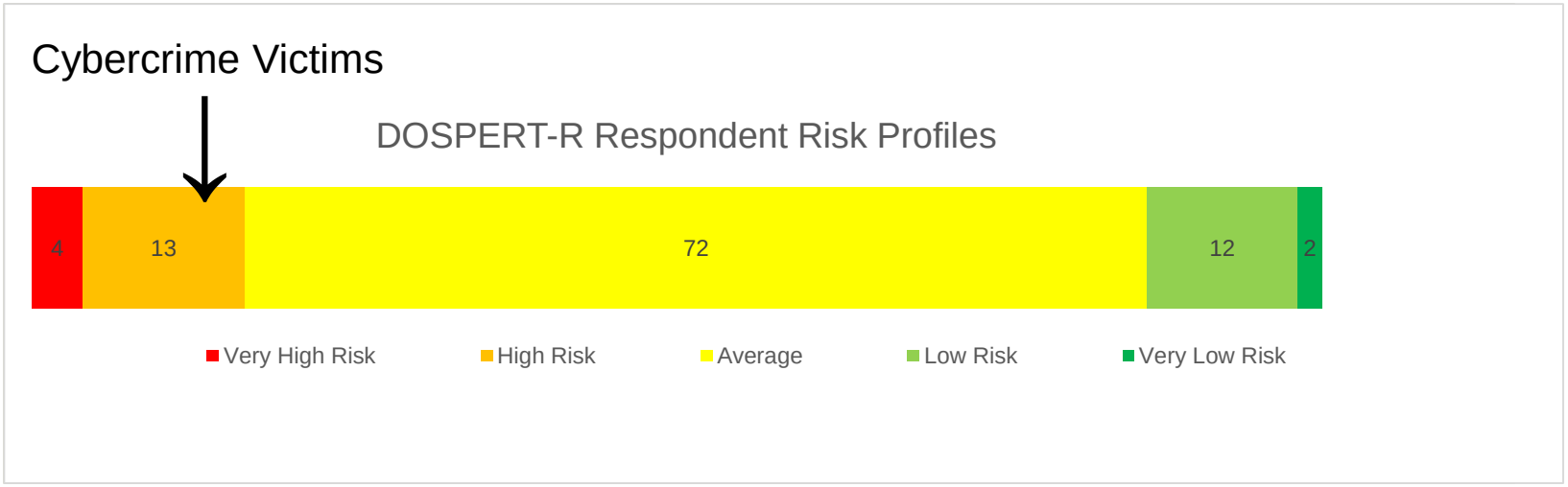
- **SeBIS *Very High Risk* individuals had been phished, had accounts hacked and suffered malware infections**
- **Two of the five had previously lost up to $500 each**

PSYCHOMETRIC PROFILING



- **CFC-F *Very High Risk* individuals reported having accounts hacked, had suffered malware infections, credit card fraud and had fallen victim to internet scams**
- **One of the four had previously lost up to $500; a second had lost up to $10,000**

PSYCHOMETRIC PROFILING



- **DOSPERT-R *Very High Risk* individuals were surprisingly resilient with 3 classified as Victors**
- **Victims were banded in the High Risk zone**

PRELIMINARY FINDINGS

- **Individuals who had suffered the highest number of incidents were more likely to smoke, take less exercise and not be saving towards their future.**
- **They were also significantly younger than the survey median age at 33.8 (*Millennials*)**
- **55% of smokers and 42% of those who did not invest in their future had suffered a financial loss, compared with a survey average of 21%**
- **50% of those unemployed and looking for work had been a victim of cybercrime and had suffered a financial loss**

VICTORS

22 VICTORS

Those who reported suffering no incidents or losses were older, predominantly female, less likely to smoke, keen investors, avid exercisers

- **4% better at online safety and security practices than the study average; slightly more future focused; 9% lower risk appetite than study average**
- **68% female**
- **9% smokers**
- **95% invested in their future**
- **On average they spent 3hr 40m exercising**
- **Median age was 49.4**

VICTIMS

20 VICTIMS

Those who had lost money were more likely to be smokers, not actively investing, risk takers by nature

- **Less confident at online safety and security practices than the study average, scoring 10% below the Victors. Risk appetite 16% higher than the Victors**
- **60% female**
- **25% were smokers**
- **Exercised 20% less than Victors**
- **42% did not invest in their future**
- **Three were retired, three unemployed and seeking work**
- **Median age was 47.6**

NEXT STEPS

First two scales offer good ‘predictive’ insights into security knowledge and ability and future focused behaviour - Very High Risk (VHR) people are ‘correctly’ identified to some extent as victims of cybercrime

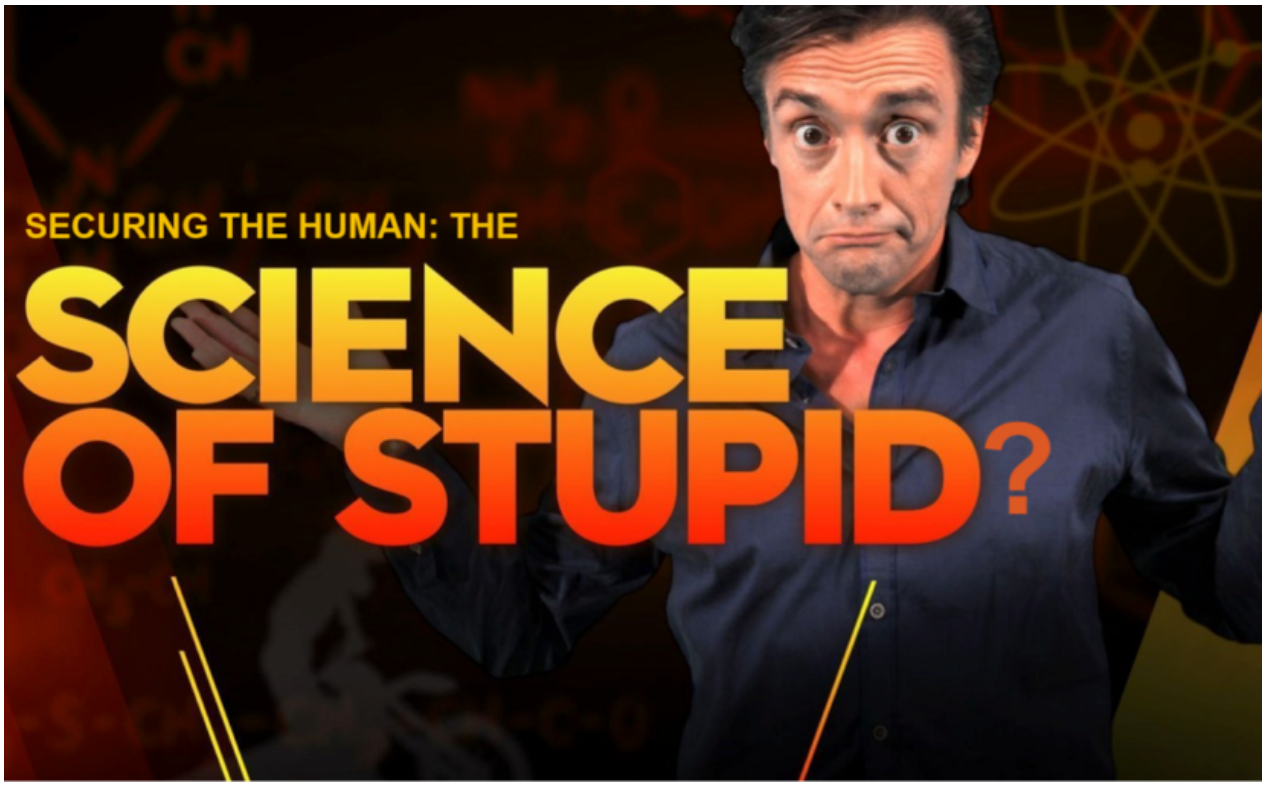
For DOSPERT-R, there appears to be a sweet spot at the start of the High Risk band; VHR recreational risk takers identified by the DOSPERT-R scale appear to be resilient ‘Victors’

Combining the three pre-existing scale scores via weighting or other means is required to produce a Security Quotient metric

University expertise will help validate these preliminary findings (potential linear / logistic / multinomial regression)

Small sample size is an issue, a larger survey dataset is necessary to validate the concept – explore large employers and IDI data

A larger dataset could allow nationality to be assessed for evaluation of Hofstede cultural ‘Individualism’ being a protective/risk factor



Securing the Human: The Science of Stupid?

Security Quotient: Preliminary Research Results

A big thank you goes to the ISACA Auckland board for the invite last week to present an update on my two year passion project to mitigate the harm caused by cybercrime.

As I noted on the day, the rather provocative session title – using the S word and TV show imagery – was chosen to keep people engaged for the always difficult post-lunch slot when audiences are fighting the urge to drift off into a light snooze as the body focuses on physical rather than mental digestion.

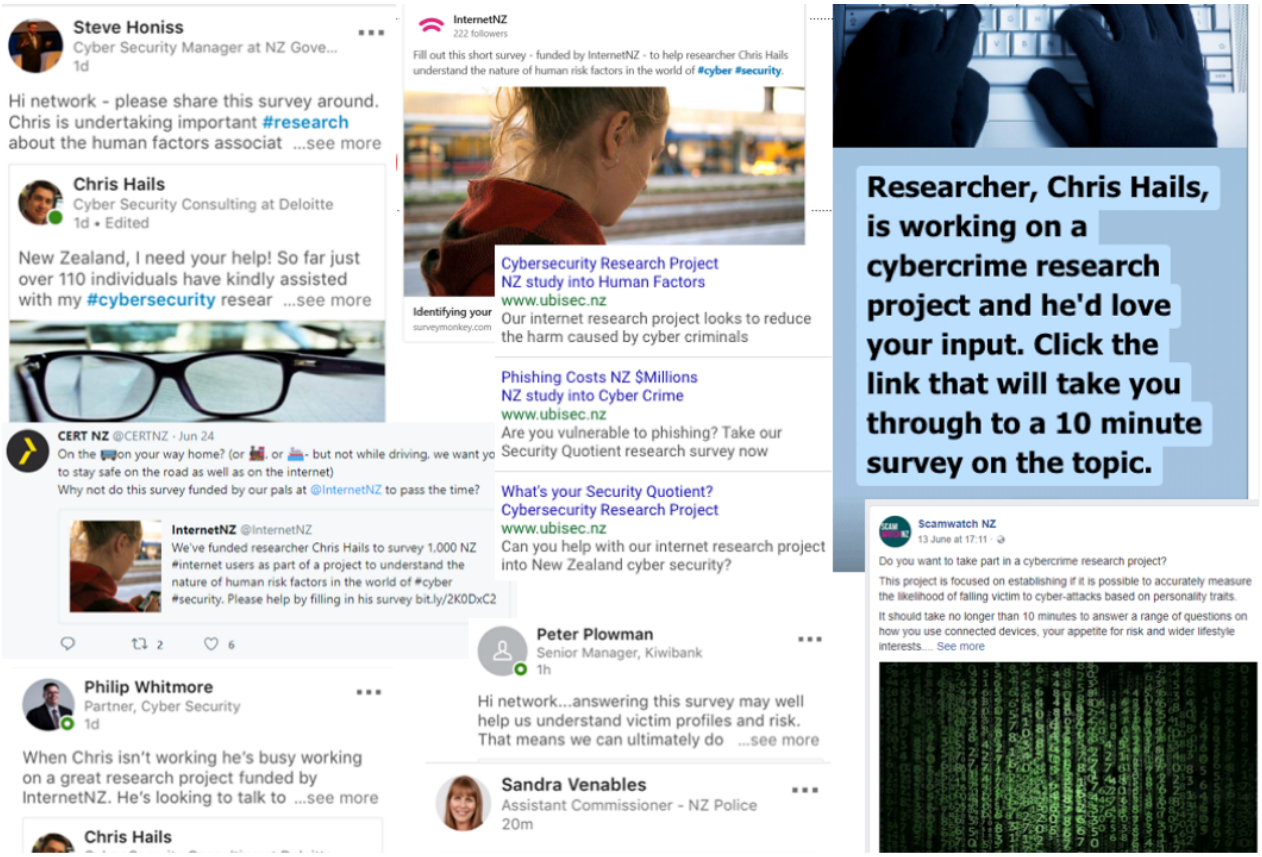
Presenting on the day felt like coming home – I originally gave a presentation at the November 2016 ISACA Cybersecurity Day on the need to move away from a model of being

the ambulance at the bottom of the cliff and increasingly targeting prevention and intervention efforts towards a subset of individuals who may be at the greatest risk of falling victim to cybercrime and common socio-technical internet attacks like phishing.

Six years spent listening to horror stories around small businesses impacted by ransomware or Business Email Compromise incidents or of individuals emotionally and financially harmed by romance and investment scams has provided the drive to get this far and I hope the insights shared were of some interest to the audience.

The SeBIS and CFC-F scales appear to offer good 'predictive' insights where there's a correlation with internet safety and security knowledge/ability and future focused behaviours. Eleven 'Very High Risk' (VHR) individuals were identified in the survey data, including four previous cybercrime victims who had lost up to $10,000. Combining the three scale scores via weighting or other means is now required to produce a final *Security Quotient* metric.

Thank You!



I owe a big thank you to all those who took the time to help promote the Security Quotient survey earlier this year to their networks and especially to those individuals who took the time to complete the survey and provided the very important data to draw from.

After promotion via mainstream and social media, through Google and Facebook PPC campaigns (thanks CFFC!), 167 responses were received. I will now be working with the University of Auckland to validate the preliminary findings I presented on identifying Very High Risk individuals via psychometric scales and the 'Victor' and 'Victim' clusters of behaviours.

Combining Safety and Security

As security professionals, we focus much of our efforts on securing data and devices, using risk assessments and security controls to protect information and information systems to provide confidentiality, integrity, and availability, to protect corporate reputations and share prices, to comply with standards and regulations, and to avoid punitive fines (#GDPR).

In this environment, end users – the 'people' in the three pillars of infosec – are often viewed as the weakest link in the security chain, too stupid, incapable or uninterested to count for much in a security programme, viewed often as a burden rather than a force multiplier to leverage when developing a stronger security culture.

The Security Quotient project has been firmly about securing and safeguarding people and to move on from a mindset of victim blaming.

What struck me last Thursday at the ISACA 2018 Cybersecurity Day was how the security world is evolving and how our historic focus on data and devices is also evolving to reflect the changing nature of technology itself and the increasing likelihood of harm potentially being caused by cyberphysical incidents and events.

Richard Harrison spoke about current and future digital crime in a healthcare context, of our increasing reliance on the integrity of data from connected medical devices and the future of healthcare implantables where cybersecurity will apply not just to connected devices but to connected people too.

John Martin's talk on the current and future states of IoT illustrated how diverse standards and a lack of comprehensive guidance and regulation is leading to increasing risk as we connect anything and everything to the internet with little effort made to include security by design or default.

And, of course, Chris Roberts' fantastic presentation on plane, train and agricultural cybersecurity was supplemented by his research into weaponising nanotechnology, hacking the human and how 'brainwave' authentication is only years away.

Next Steps

I remember being asked whilst interviewing for Deloitte “what is your proudest work achievement?” and talking about the development and operation of the ORB reporting platform. From small beginnings in August 2010 through to August 2016, the system enabled New Zealanders to report almost 28,500 incidents and record $35m in direct financial losses.

The platform provided a real time reporting dashboard and allowed partner agencies to stay up to date with incident trends; writing monthly intelligence reports for partners delivered a picture of the harm across NZ and allowed targeted educational resources to be focused where required.

I’ve taken the learnings from this experience at the bottom of the proverbial cyber incident cliff and want to build something that delivers an opportunity to prevent further harm from being caused to the most vulnerable. In a Security Quotient ‘product’ roadmap, now would mark the end of the Alpha phase with this harm reduction vision validated through prototyping and a Minimum Viable Product defined.

If the model can be assessed further with assistance from the University of Auckland, it should be possible to deliver a Quotient value through an online service that presents both a risk rating and guidance to the user at the end of the survey.

My next aim – *after rapidly writing up the research completed to date* – will be to build a 'human vulnerability scanner' on a par with the likes of Nessus or Qualys which work to identify risks through CVSS scores. If the Security Quotient predictive model can be further validated through statistical analysis, developing an online platform will give me a chance to return to delivering digital tools that provide real value to the user.

Ultimately, it would be great to also develop a 'human firewall' capability in the form of targeted education and/or an operating system with individualised, adaptive security that can wrap a more effective safety net around the internet user.

With cybercrime now more lucrative than the global drugs trade, developing predictive analytics to prevent internet users from falling victim seems more important than ever.

Can you help?

There's no doubt that the small dataset is an issue for validating the predictive nature of the Security Quotient metric. If you're a CISO, CSO, ISM or security practitioner interested in the concept and able to assist with getting a large NZ workforce involved, do please reach out: research@ubisec.nz.

Connecting to a current security culture programme or large phishing simulation dataset would be an interesting next step too.

A larger dataset could also allow respondent nationality to be assessed for evaluation of Hofstede's cultural 'Individualism' measure as a protective/risk factor.

October 22, 2018 ubisecusr