UNIVERSITY OF TWENTE.

HOW ICT CHANGES VICTIMIZATION

OCTOPUS CONFERENCE ON COOPERATION AGAINST CYBERCRIME

17 TO 19 JUNE 2015 IN STRASBOURG, FRANCE

WORKSHOP 3: VICTIMS OF CYBERCRIME – WHO CARES?

MARIANNE JUNGER

M.Junger@Utwente.nl
http://www.utwente.nl/bms/iebis/staff/junger

HOW ICT CHANGES VICTIMIZATION

1. Victim characteristics are changing under the influence of ICT
2. The impact of victimization is not less than ‘traditional crime’
3. To protect humans against scams is hard
   - more research and experimenting is necessary

DEFINING CYBERCRIME IS WORK IN PROGRESS

1. Broad concept
   - *Crimes against computers*
   - *Crimes using*
   - *Crimes 'in' computers*

2. Legal definition is handy. See Budapest convention
   - Bullying

3. No agreed definition
   - Prevalence rates of victimization vary wildly

PREVALENCE: 12 RANDOM SAMPLES

1. Europe: Special Euro-barometer commissioned by the European Commission (TNS Opinion & Social, 2012)

2. England and Wales: two waves of the Crime Survey for England en Wales (CSEW) (Lader, Hoare, & Ivy Laumann, 2012) and (McGuire & Dowling, 2013)

3a. The Netherlands: The Safety monitor (Statistics Netherlands, 2013)

3b. The Netherlands: Victim survey (Domenie, Leukfeldt, van Wilsem, Jansen, & Stol, 2013)

3b. The Netherlands: LISS panel (van Wilsem, 2013a, 2013b)

4a. US: National Crime Victimization Survey (NCVS) (Harrell & Langton, 2013)

4b. US: Competitive Edge (Nienstadt, 2009)

4.c US: National Public Survey on white collar crime (Rebovich, Layne, Jiandani, & Hage, 2000)

5. Canada: General Social Survey (GSS) (Perreault, 2011)

6a. New Zealand: The experience of E-crime. Findings from the New Zealand Crime & Safety Survey 2006 (Mayhew & Reilley, 2007a)

6b. New Zealand: Statistics New Zealand (Statistics New Zealand, 2006)

7. Australia: Identity crime and misuse in Australia: Results of the 2013 online survey (Smith & Hutchings, 2014)

PREVALENCE CYBERCRIME VICTIMIZATION , MAXIMUM %

MEASURING CYBERCRIME - ISSUES

1. Prevalence rates relatively high
2. In addition to usual methodological issues
   - How to define?
   - How to ask the right question?
   - Do respondents know about a virus, being hacked, etc.?

ARE VICTIMS AND OFFENDERS' CHARACTERISTICS CHANGING?

STUDY

1. Police records
2. Sample: a-select
   - East of the Netherlands
   - Threats (n=300)
   - Frauds (n=300)
3. Amount of ICT

Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? *European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37.*

CYBER CHANGES OFFENDERS

Offenders of cybercrime tend to be

- Younger (fraud)
- Female (threats)
- **Born in NL (fraud, *)**
- **Paid job (threats, *)**
- **Less often criminal record (threats, *)**

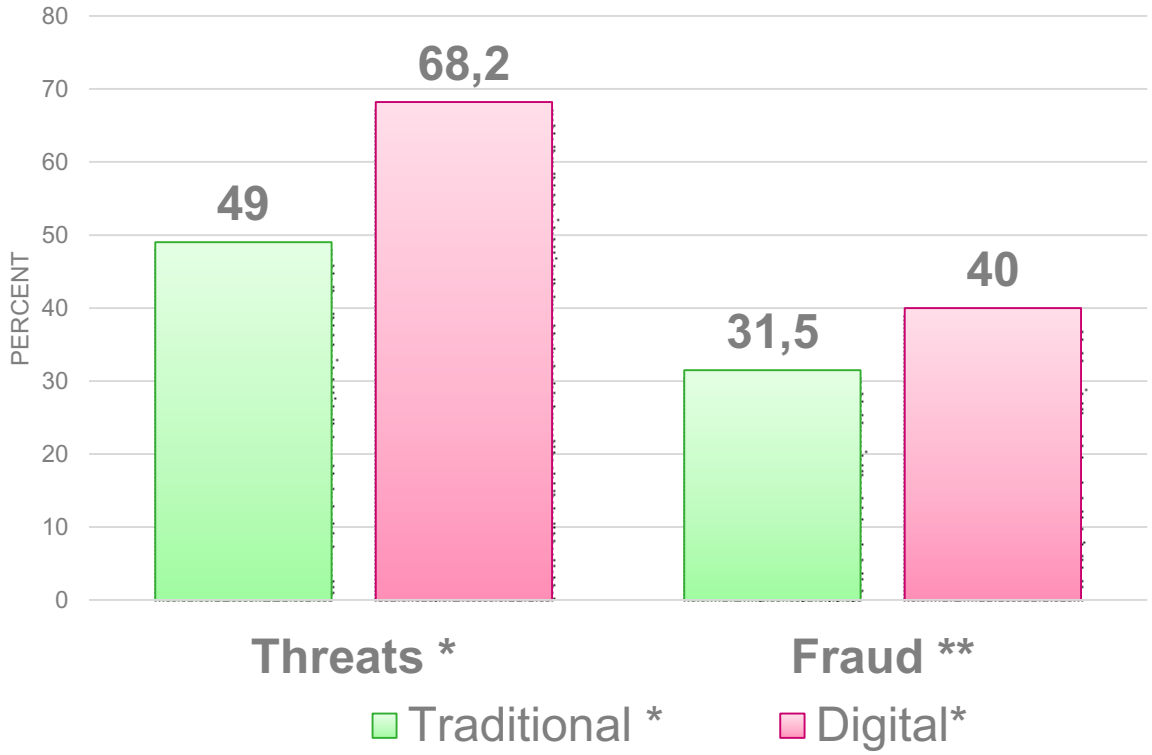
Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? *European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37.*

CYBER CHANGES VICTIMS

Victims of cybercrime tend to be:

- Female (threats & fraud, both *)
- Born in NL (threats, *)
- but age is similar

Female victims of threats & fraud, of traditional and digital crime



SUSPECT-VICTIM RELATIONSHIP IN TRADITIONAL & DIGITAL OFFENSES, IN %

	Threats			Fraud		
	Traditional	Digital		Traditional	Digital	
Business associates/employee	5.2	2.2		**24.0**	**47.3**	***
Family	8.2	8.9		1.2	0.9	
Ex-partners	**15.5**	**28.9**	*	**3.5**	**-**	*
Chat friends	**-**	**4.4**	**	0.6	0.9	
Other relationship	7.8	13.3		**5.3**	**0.9**	*
N	232	45		171	112	

Montoya, L., Junger, M., & Hartel, P. (2013). How 'Digital' is Traditional Crime? *European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37.*

IMPACT OF CRIME VICTIMIZATION – IN GENERAL

1. Shock and a loss of trust/faith in society
2. Guilt
3. Physical injury
4. Financial loss
5. Psychological effects
6. Social effects
7. Consequential effects: changes in perceived risk of future victimisation.
   - Repeats
   - Changes in fear of crime
   - Propensity to take additional crime preventive measures, which themselves have financial costs

Shapland, J., & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology, 14(2), 175-217.*

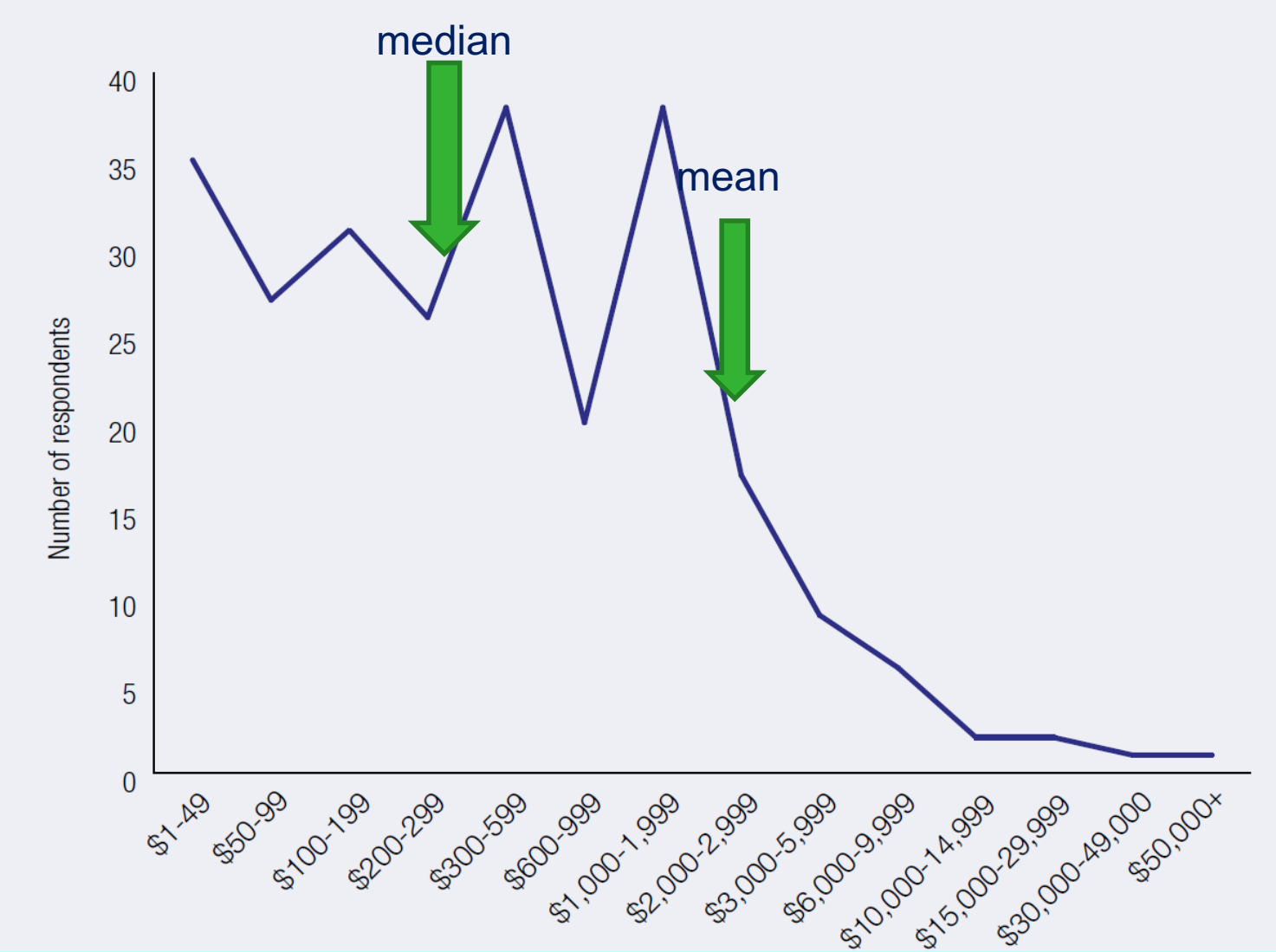
IMPACT OF CYBERCRIME VICTIMIZATION

IDENTITY THEFT

1. Direct financial loss
2. Indirect financial loss
3. Lost income and opportunities due to tarnished

Lawson, P. (2009). Identity-related crime victim issues: A discussion paper. *Commission on Crime Prevention and Criminal Justice, 18th session. Accessed May, 13, 2011.*
Lawson, P. (2011). *Responding to victims of identity crime : a manual for law enforcement agents, prosecutors and policy-makers. Vancouver, BC: International Centre for Criminal Law Reform and Criminal Justice Policy. http://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn28623-eng.pdf.*

FINANCIAL LOSSES OF IDENTITY THEFT – LAST YEAR



Smith, R. G., & Hutchings, A. (2014). Identity crime and misuse in Australia: Results of the 2013 online survey (Vol. 128). Canberra, Australia: Australian Government. Australian Institute of Criminology. http://aic.gov.au/media_library/publications/rpp/128/rpp128.pdf.

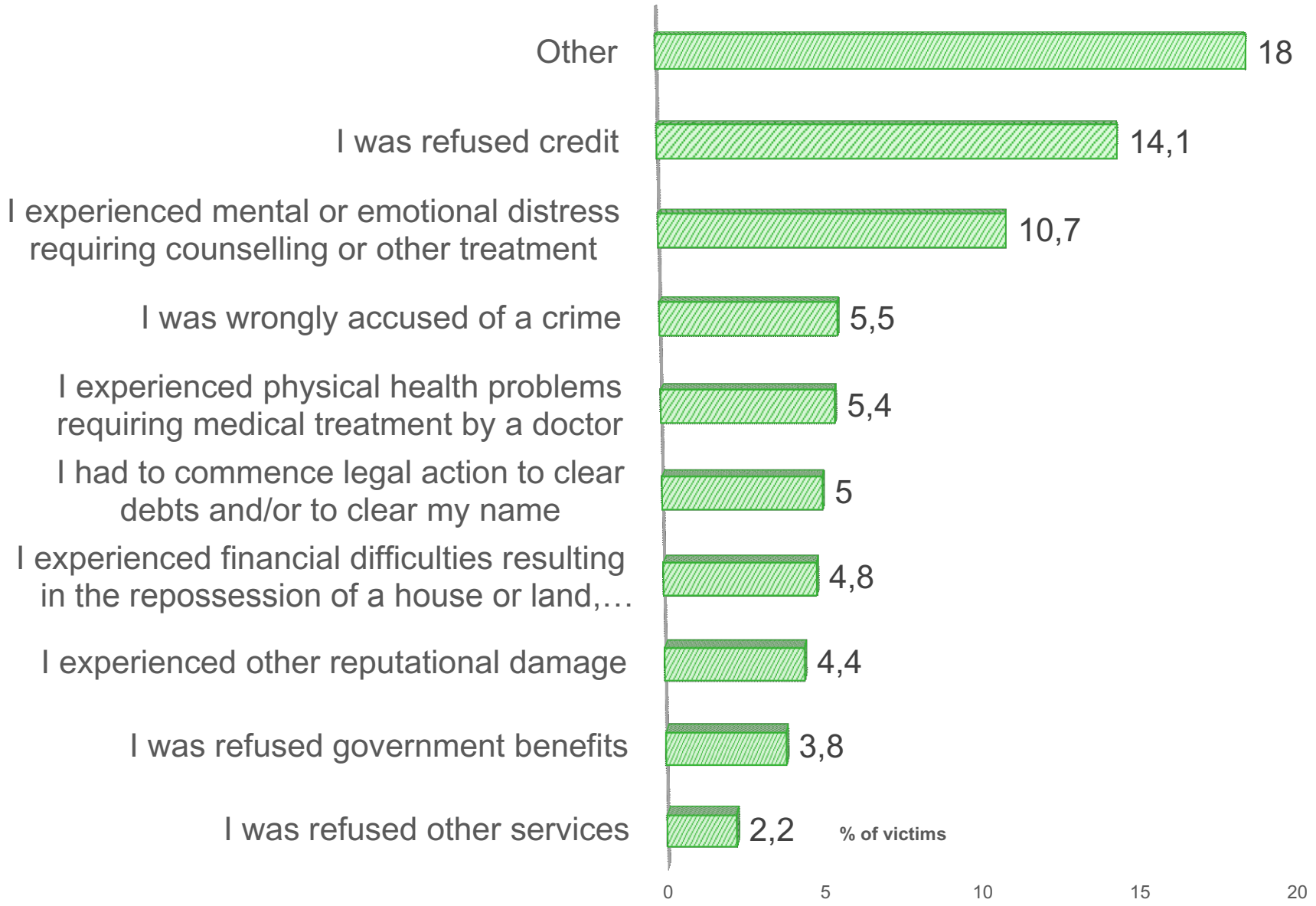
IMPACT OF CYBERCRIME

IDENTITY THEFT

4. Time and effort to restore identity information and reputation;
5. Harassment by creditors, debt collectors or law enforcement;
6. Social consequences. Loss of family and social support, as a result of the false accusations and reputational damage
7. Emotional and psychological trauma
8. Physical impact

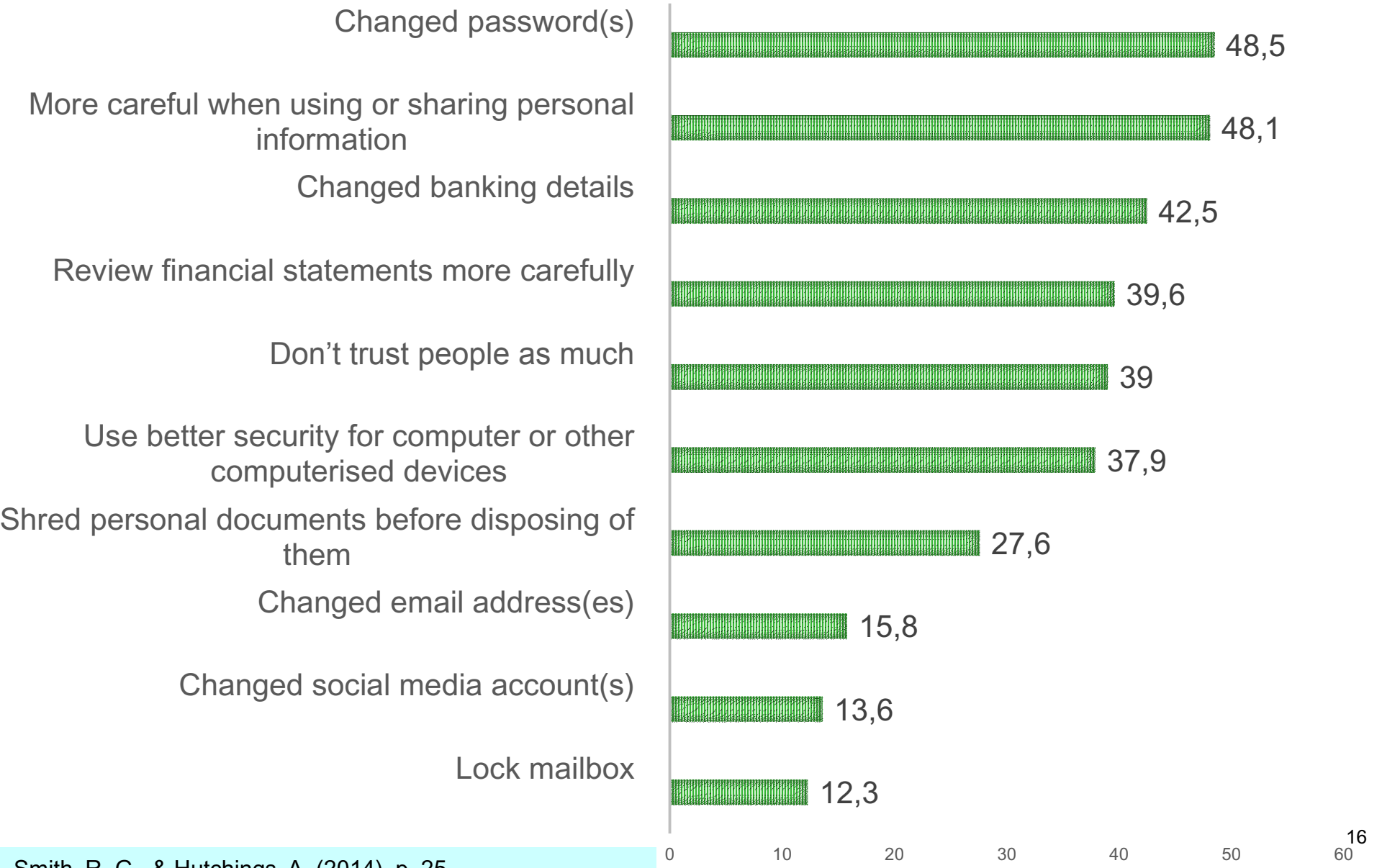
Lawson, P. (2009). Identity-related crime victim issues: A discussion paper. *Commission on Crime Prevention and Criminal Justice, 18th session. Accessed May, 13, 2011.*
Lawson, P. (2011). *Responding to victims of identity crime : a manual for law enforcement agents, prosecutors and policy-makers. Vancouver, BC: International Centre for Criminal Law Reform and Criminal Justice Policy. http://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn28623-eng.pdf.*

CONSEQUENCES OF IDENTITY THEFT IN PREVIOUS YEAR, N=460



Smith, R. G., & Hutchings, A. (2014), p. 21

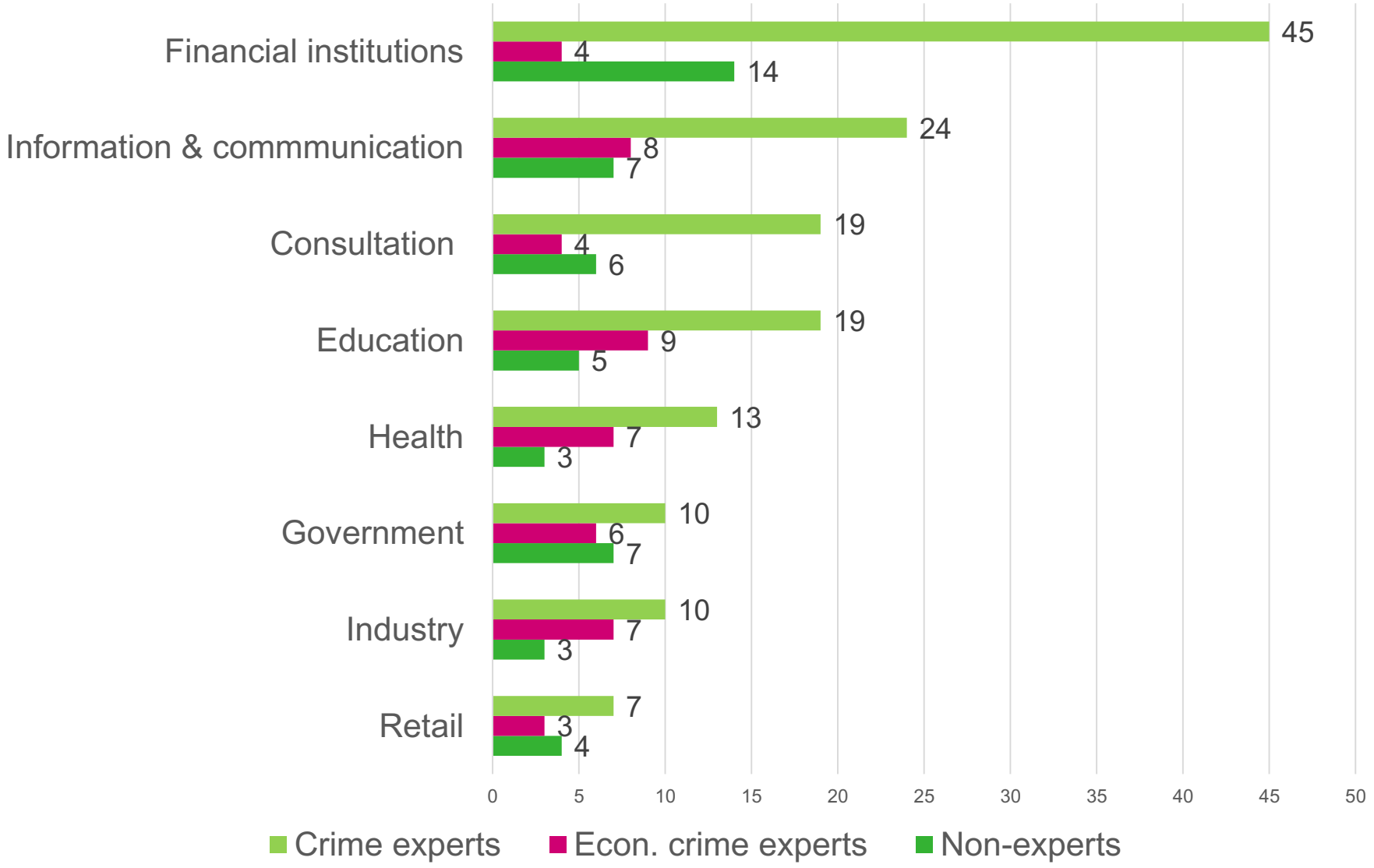
MAIN BEHAVIOURAL CHANGES AS THE RESULT OF IDENTITY THEFT IN PREVIOUS YEAR, IN %, N=460



Smith, R. G., & Hutchings, A. (2014), p. 25

ORGANIZATIONS AS VICTIMS

PREVALENCE OF CYBERCRIME BY ECONOMIC SECTOR AND EXPERTISE, THE NETHERLANDS



PwC. (2014). Cybercriminaliteit tegen Nederlandse organisaties: een digitale dreiging. In Price Waterhouse Coopers (Ed.). Den Haag, NL

IMPACT OF CYBERCRIME ON THE COMMUNITY

1. Loss of online business and consumer confidence in the digital economy
2. The potential for critical infrastructure to be compromised
3. Costs to government agencies and businesses in re-establishing credit histories, accounts and identities
4. Costs in order to improve cyber-security measures
5. Fuelling other criminal activity
6. Costs in time and resources for law enforcement agencies.

REPORTING TO THE POLICE

SECONDARY VICTIMIZATION

Identity theft - Australia:

1. No one 9%
2. friend/family 54%
3. Government/business 8%
4. Both friends/family & government business 30%

5. Most were satisfied

Smith, R. G., & Hutchings, A. (2014), p. 23

THE CHALLENGE

Can we protect victims?

VULNERABILITY FOR SCAMS

- WE WERE BORN TO TRUST

CAN HUMANS BE PROTECTED AGAINST SCAMS?

1. https://www.youtube.com/watch?v=opRMrEfAIiI

HOW VULNERABLE ARE POTENTIAL VICTIMS?

EXPERIMENT IN ENSCHEDE - NL

Two page questionnaire

Conditions

1. Questionnaire
2. Questionnaire & ‘awareness questions’ on cybercrime experience
3. Questionnaire & ‘warning’

UNIVERSITY OF TWENTE.

HOW VULNERABLE ARE POTENTIAL VICTIMS?

EXPERIMENT IN ENSCHEDE - NL

Questions

1. Will people give us their email address?
2. The kind of product the respondent bought online
3. The web shop they used
4. Will people give figures of bank account?:
5. SUM: The combination of information could be used by attackers

Overink, F.-J. (2015). *Should Interventions be Prevented? A Research into the Right Way to Prevent People for Phishing Attacks. University of Twente, Enschede, Nl.*

SUBJECTS THAT PROVIDED INFORMATION, IN %, N=281

	Control Group	Awareness Group	Warning Group
Email filled in *	81.3	87.2	64.8
Filled in the kind of product the respondent bought online ns	84.4	83.0	81.3
Filled in the web shop ns	80.2	87.2	85.7
IBAN Usable for phishing ns	49.0	40.4	40.7
N	96	94	91

Overink, F.-J. (2015). *Should Interventions be Prevented? A Research into the Right Way to Prevent People for Phishing Attacks. University of Twente, Enschede, Nl.*

PROTECTION AGAINST SCAMS

1. Is hard
2. Don’t blame the victim! *It will not bring you closer to the solution of the problem*

SUPPORT NEEDED FOR VICTIMS OF CYBERCRIME

1. Safety - prevent repeats
2. Support
3. Information
4. Justice

Lawson, P. (2009). Identity-related crime victim issues: A discussion paper. *Commission on Crime Prevention and Criminal Justice, 18th session. Accessed May, 13, 2011.*
Lawson, P. (2011). *Responding to victims of identity crime : a manual for law enforcement agents, prosecutors and policy-makers. Vancouver, BC: International Centre for Criminal Law Reform and Criminal Justice Policy. http://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn28623-eng.pdf.*

SUMMARY & CONCLUSIONS

1. Cybercrime – no agreed definitions and measures

   A strong need for more research

   1. Demographic characteristics
   2. Repeat victimization?
   3. Time and place
   4. Where are the data on organization's victimization?
   5. What are the evidence based interventions

2. Hard to get good picture of prevalence – the threat landscape & crime victimization has changed in the past two decades

SUMMARY & CONCLUSIONS

3. Offender and victim characteristics are changing
   - Not a homogenous trend
   - We hypothesize a ‘normalization of crime’

4. By nature, humans are vulnerable and hard to protect

- More research is needed to find out how to improve protection
- Action plan to help victims is necessary

Montoya, L., Junger, M., & Hartel, P. (2013). How ‘Digital’ is Traditional Crime? *European Intelligence and Security Informatics Conference (EISIC) 2013, 31-37.*

Any questions?

M.Junger@Utwente.nl
http://www.utwente.nl/bms/iebis/staff/junger/

	1	2	3a	3b	3c	4a	4b	5	6a	6b	7
Country	Europe	England en Wales	Netherlands	Netherlands	Netherlands	USA	USA	Canada	New Zeeland	New Zeeland	Australia
Name survey, source	Eurobarometer (TNS Opinion & Social, 2012)	British Crime Survey, Two sweeps a) (Lader et al., 2012) b) (McGuire & Dowling, 2013)	Dutch Safety Monitor (Statistics Netherlands, 2013)	Victim survey (Domenie et al., 2013)	LISS panel (van Wilsem, 2013a, 2013b)	National Crime Victimization Survey (Harrell & Langton, 2013)	Victim survey (Nienstadt, 2009)	Victim survey (Perreault, 2011)	Victim survey (Mayhew & Reilley, 2007a)	Household use of information and communication technology, 2006 (Statistics New Zealand, 2006)	Identity crime and misuse in Australia: Results of the 2013 online survey (Smith & Hutchings, 2014)
Year data collection	2012	2010/11 2011/12	2012	2012	2008	2012	2009	2009	2005	2006	2013
Number of respondents	26,593 Selection internet users:18,983	a) 8,383 internet users b) 2,015 interviews, 1,518 internet users	77,989	10,314, of which 9,163 internet users	5,750 for hacking & harassment % 6,201 for online shopping fraud	69,814	1003	19422	Households: 4,229 Maori sample: 1,187	24,855 individual And 13,757 households from a larger survey completed the ICT survey	4,995
Age	15 and over	16 and over	15 and older	15 and over	16 and over	18 and older	18 and over	15 years and over	15 and over	15 and over	15 and over
Selection method	Multi-stage random selection – proportional to country size	Random locale approach. Addresses from the Royal Mail address list	Random selection of the residents of the Netherlands	Random selection of the residents of the Netherlands	Representative sample of Dutch individuals who participate in monthly Internet surveys	Nationally representative sample	Random sampling technique from a voter file	Random Digit Dialling	Nationally Stratified random sample	Sample of households, representative for New Zealand stratified[3]	Sample of households, representative for Australia
Response rate	Not available	a) 76%[1] for the BSC overall2010/11 75% for the BSC overall in 2011/12	38,4%	47.2% online	70% of the participants in the panel	68.2%	Not available	61.6%	Main[2] sample: 59%. Māori sample: 56%	Households: 94% Individuals: 89% from original survey. General survey; about 86% response[3]	na
Data collection	Face-to-face or CAPI (Computer Assisted Personal Interview)	Face-to-face	45% Online, and – after reminders, written questionnaire filled in at home by 55%	25.7% Online. 17.3% telephone interviewing. 1.1% written questionnaire filled in at home	Online	Computer-assisted personal interviewing (CAPI) or Computer-assisted telephone interviewing	Telephone	Computer-assisted telephone interviewing (CATI)	Face-to-face	Face-to-face combined with telephone	Online survey

Australia: (Smith & Hutchings, 2014)

Identity theft: Misuse of personal information was defined as obtaining or using personal information without permission, to pretend to be the person in question or to carry out a business in that person's name without their permission, or other types of activities and transactions. The use of personal information for direct marketing, even if this was done without permission, was excluded.

Misuse of various types of personal information. This was defined as including misuse of an individual's name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (eg fingerprint), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student number, as well as other types of personal information.