WARWICK

ecrime

The Economic Impacts of Cyber Crime

Human Factors & Successful Implementation of Awareness Campaigns

Introduction

- It is widely acknowledged that there is a human aspect to cybercrime. The norms, values, and behavioural dispositions of employees and end-users can effect the risk of a cybercriminal incident occurring.
- This raises the prospect of managing cybercrime by trying to change the norms, attitudes, and dispositions of employees and users.
- However, it is an obvious fact that an individual's norms, attitudes and behavioural dispositions are going to vary at least to some extent from culture-to-culture.

Awareness Campaigns

- An awareness campaign is a programme enacted by an organisation or government which is intended to make a targeted group of individuals (often end-users) aware of some variety of cybersecurity risk, and persuade them to engage in counteractive or pre-emptive behaviour.

The Structure of an Awareness Campaign

The Programme Host. This is the party or set of parties responsible for devising and running the programme.

The Target Group. This is the group of people which the awareness campaign sets out to influence. Often this is end-users, but it could be the employees of an organisation.

The Desired Behavioural Change. This is the set of security-conducive norms, values, or behavioural dispositions the programme host is seeking to persuade members of the target group to adopt.

The Content of the Programme. This is the set of elements that constitute the programme (e.g. adverts, websites, leaflets); the information contained in the programme (e.g. how to spot tell-tale signs of the criminal event occurring, how to go about counteracting the risk, where further information might be sought); and the persuasive techniques used (e.g. use of testimony by experts, an appeal to fear of losing sensitive information, the use of humour, an appeal to norms or values already held by the target group).

Hofstede's Cultural Dimensions Theory

- Hofstede identifies six dimensions along which the culture of a given group might differ.
- I'll examine each in turn, before making some comments about how differences along these dimensions might have an impact on the success of an awareness campaign.

Power Distance, Individualism, Masculinity

Power Distance. Some individuals in a society have more power and more opportunity than others. Power distance measures to what extent the individuals with less power are willing to tolerate this state of affairs. A high score on the power distance dimension indicates a high degree of toleration, a low score low toleration.

Individualism. Do the members of the society think of themselves as only having an obligation to look after themselves and their own, or do they have a more communitarian outlook? A high score on this metric indicates the former attitude, a low score the latter.

Masculinity. Certain norms and values are typically classified as masculine. Examples of such values include achievement, heroism, competitiveness, assertiveness, material reward for success, and being the best in a particular field. A high score on this metric indicates a preference for masculine values, a low score for a different set of values.

Uncertainty Avoidance, Long-Term Orientation, Indulgence

Uncertainty Avoidance. The future is often difficult to discern, new people difficult to read, and new situations difficult to navigate. This can generate anxiety on the part of the individual, but alternatively the individual might have a relaxed, fatalistic attitude towards it. A high score on this metric indicates a preference for the avoidance of uncertainty, a low score indicates the more relaxed attitude.

Long-Term Orientation. Societies have traditions which over time might get broken down, modified, or replaced. This dimension of cultural difference measures the extent to which members of a particular culture feel that such change is intrinsically bad. A high score on this metric indicates a relaxed and progressive attitude towards such cultural changes, a low score indicates the opposing attitude.

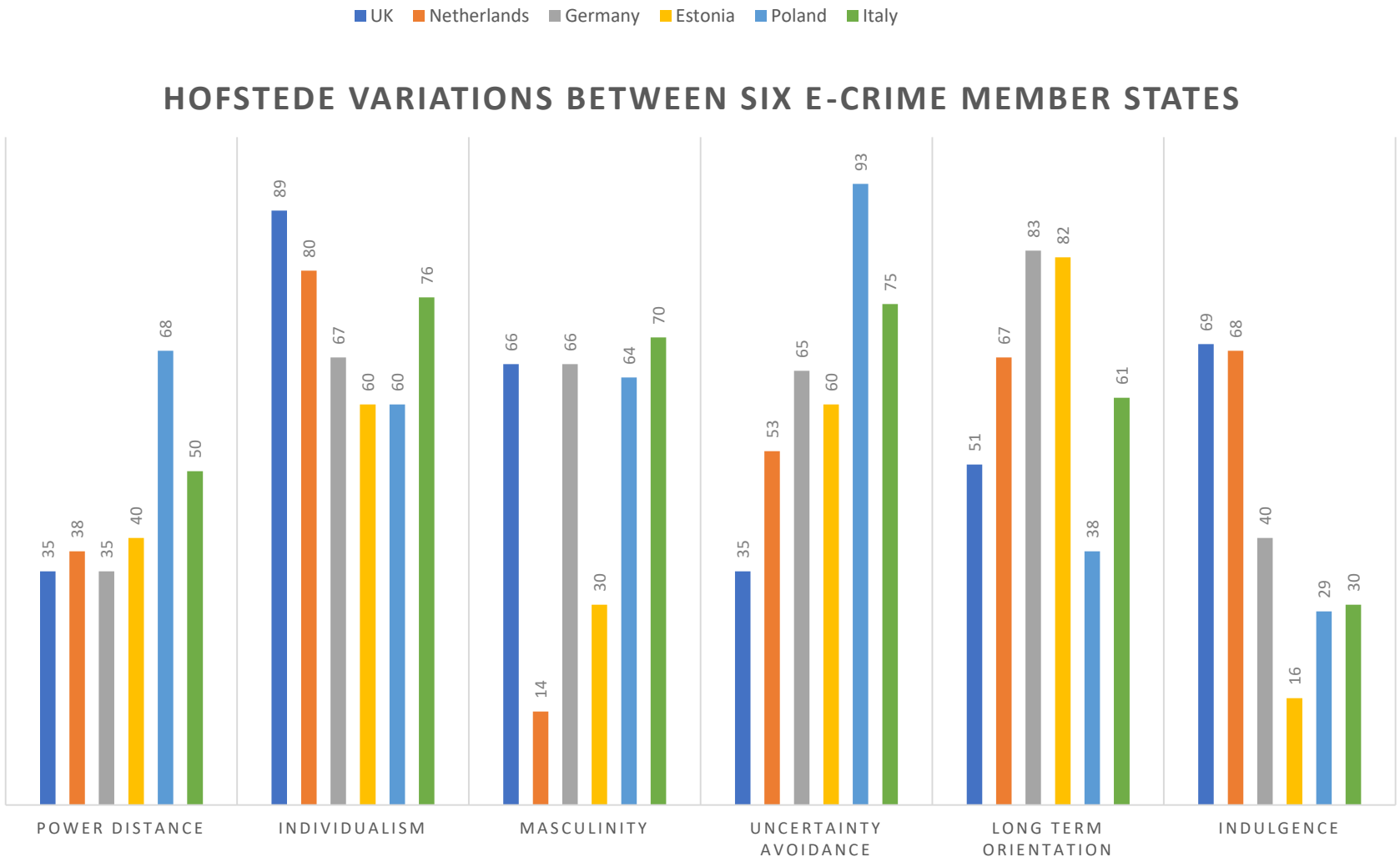
Indulgence. Is living the good life a matter of indulging our passions, desires and projects or does it rather involve control, restraint, and a respect for duty? A high score on this metric indicates an indulgent society, a low score a restrained one.

The Effect on Awareness Campaigns

- How might differences between societies along Hofstede's six dimensions have an effect on the success a cybersecurity awareness campaign? Let us pick on two examples:

Individualism. If a society scores low on the individualism parameter, then the recommendations given by the awareness campaign could be cast as something that it is one's civic duty to do. If the society is individualistic, however, then the awareness campaign might talk about the risk posed to the individual and their family. Indeed, rights like privacy and non-interference in general will be assigned special importance in individualistic societies. Simply emphasising that cybercrime is intrinsically a violation of those rights will therefore be effective. Not so if the society is non-individualistic.

Masculinity. If a society scores high on the masculinity parameter, the state protection strategies discussed as part of the awareness campaign could be presented as something that it is necessary to do in order to secure success in one's career. Protection of data could be represented as a competition between the user and the prospective criminal.


UK
Netherlands
Germany
Estonia
Poland
Italy
HOFSTEDE VARIATIONS BETWEEN SIX E-CRIME MEMBER STATES
35
38
35
40
68
50
89
80
67
60
60
76
66
14
66
30
64
70
35
53
65
60
93
75
51
67
83
82
38
61
69
68
40
16
29
30
POWER DISTANCE
INDIVIDUALISM
MASCULINITY
UNCERTAINTY AVOIDANCE
LONG TERM ORIENTATION
INDULGENCE

High-Level Roadmap For Sector Specific Countermeasures As Solution Portfolios

General Recommendations

There are several general recommendations which cut across all sectors:

- Better perimeter and service knowledge
- Prioritize Patch management
- Reduce complexity and opportunities
- Strengthen internal collaboration
- Increase education and training
- Use of Honeypots (often underestimated)
- Use of disinformation and deception
- Knowledge of your enemies
- Hack yourself
- Strengthen integration and data traffic analysis
- Build a security in-house capability:
- Limit the BYOD
- Strengthen external architectures
- Moving target architectures

Sector-specific: *retail*

Recommendations for: *individuals*

- Use strong passwords with multi-factor authentication.
- Take heed of awareness programmes and trust initiatives enacted by the relevant organisation.
- Ensure that the organisation being relied on is compliant with the PCI (Payment Card Industry Data Security Standard).

Sector-specific: *retail*

Recommendations for: *companies*

- Keep Operating Systems patched and all software updated, including anti-malware solutions.
- Implement end-to-end encryption to the payment process.
- Use a next-generation firewall that implements intrusion prevention system (IPS).
- Use a misuse detection approach to detect cyber-attacks, for example: make use of the set of attack signatures in the intrusion detection system.
- Adopt a security policy that trusts nothing (networks, resources, etc.) and no one (vendors, internal personnel, etc.), and then work by adding needed exceptions.

Sector-specific: *retail*

Recommendations for: *companies*

- Organizations that handle payment systems should comply with standards, such as PCI-DSS. These standards provide a widely accepted set of effective policies and procedures that aim to reduce the exposure of companies to cyber-attacks.
- Adopt new secure technologies such as the EMV payment card technology.
- Train internal personnel making employees aware of cyber threats, security rules, and threat actors TTPs (Techniques, Tactics, and Procedures).
- Be complaint with the PCI (Payment Card Industry Data Security Standard)
- Periodically conduct vulnerability assessment and penetration tests on your platform.
- Secure your infrastructure by adopting a layered defence model that puts together several components, including firewalls, intrusion detection systems, and physical network segregation.

Sector-specific: *retail*

Recommendations for: *national/EU level*

- Encourage information sharing with respect to cyber intelligence and best practices under the platforms created by the NIS Directive.

- Improving awareness and education on cybersecurity especially among SMEs. Awareness programmes are explored in more detail in the following part of this report.

- Encourage taking out cyber insurance in a voluntary manner.