Social and Behavioural Techniques to Boost Awareness

Carlos Orozco Corona and **John Austen** argue that security awareness programmes work better when everyone is involved in the process. They outline a plan to make it happen.

Royal Holloway
University of London

SearchSecurity.co.UK

HOME

BEHAVIOURISM AND GROUP COMMUNICATION

SOCIAL NETWORK ANALYSIS

OUTLINING THE CAMPAIGNS

COMMUNICATION CHANNELS

STRATEGY SUMMARY

SOURCES

THIS PAPER DISCUSSES the issues of human behaviour in relation to Information security awareness programmes and recommends a more holistic approach to their design and delivery. Other current research in this area recommends invoking a multidisciplinary approach to the conception of these programmes by bringing in the skills of psychologists, behaviour analysts, sociologists and philosophers to add those of information security practitioners and researchers.

This approach to the construction and delivery of awareness programmes is aimed at a wider and broader understanding of human behaviour in the workplace, with the aim of capturing innovative ideas from staff and employees within an organisation and applying them effectively. Whilst this concept may in a number of ways be seen to be hypothetical and suggestive, it does have the advantage of assessing human reaction to security concepts.

From various studies and surveys of existing awareness programmes it has been seen that there are common problems when measuring their effectiveness. These can be summarised under the headings below:

1. Management Support

If senior management are not seen to be either directly involved or supporting these programmes financially or with sufficient resources, or fail to provide specialist awareness and educational materials, then there is a perception amongst users and employees that information security of less importance.

2. Security Policy Objectives

If the policy objectives in awareness programme or campaign are confused, or not clear, then like a cascade, the messages within the programme will lack the necessary impact.

3. The Security Management Framework

If the security management framework is informal or lacks meaningful documentary procedures, then there can again be a perception amongst staff that information security is more optional than mandatory.

4. Measuring the Effectiveness of Awareness Programmes or Campaigns

Surveys suggest that too much emphasis has been placed upon measuring the effect of security campaigns by pure statistical results. Trying to innovate ideas from employees makes them feel more inclusive in the process rather than making it just a test of obedience.

DECISION PROCESSES—TRYING NEW IDEAS

The terminology of an Innovating Decision Processes relates to an approach whereby the emphasis in addressing and conceiving information security awareness programmes (ISP's) starts with the skills and capabilities of the subjects (or the receivers, users or employees), rather than pure organisational agendas. By starting with an investigation of the current knowledge, skills and capabilities of the subjects, the process can make more informed decisions on how individuals perceive reality, (or real security issues), which is an important part in disseminating information in the security campaign. The advantage of this approach, prior to any decisions being made, is that there is a need to have positive effects and exert influences on the attitudes of individuals by assessing their ability to cope with and understand the issues at stake. By taking this dynamic into account at the initial stage, the awareness programme or campaign can then be processed to match the security needs of the organisation.

THE ISSUES OF BEHAVIOURISM AND GROUP COMMUNICATION

Psychologists tell us that individuals can be heavily influenced by the actions and thought processes of those within their own social network. Communication between those in a social network can lead people to behave in a determined manner. Taking this a stage further, social psychology is behaviour applied in a social learning environment – and this can be a workplace environment where employees establish communication channels. Account also needs to be taken of cognitive behavioural actions which relate to the use of reasoning, intuition or perception of individuals who may have already established beliefs, feelings or attitudes. Lewin's Force Field Analysis (named after Kurt Lewin the German-born psychologist) analyses social reactions by advising that when there is a motive to achieve a goal there are some forces which help (advantages) and some which block (disadvantages). Amongst the many decisions that individuals take, if an awareness programme is perceived as a 'helping force' it has a greater chance of success.

Group Communication refers to social behaviour where individuals within a group act upon the same information. If there is communication between them, then there is a greater likelihood of a mutual understanding that can lead to common agreement and, ultimately, to collective action. Take the situation whereby person 'A' communicates some information to person 'B'. 'B' normally enters into a personal, subjective and sometimes biased interpretative process. Included in this interpretation are prior conditions or known factors which influence this interpretive process. By applying Lewin's 'force field' analysis model, these prior conditions will be interpreted as either 'helping' (or driving) forces, or 'blocking' (or resisting) forces. The tilting balance of this interpretation will lead to either a positive or a negative attitude to the information that has been shared. This attitude will in itself become a prior condition and may influence any further interpretation unless there is a reverse communication channel back to 'A'. By constant communication there is more chance of leading to the process of:

a) mutual understanding;
b) mutual agreement; and
c) collective action

Several studies support the existence of informal communication roles. Some individuals are natural communicators ('bridges') and have a cosmopolitan attitude to their colleagues. Other individuals are 'opinion leaders' – with an ability to exert a certain level of influence over their peers. Therefore, identifying 'bridges' and 'opinion leaders' is a prime objective of 'change agents,' as these individuals can be employed to initiate the epidemic behaviour to spread information across an organisation. This is supported by 'Pareto's Law (otherwise known as the 80%-20% rule). A generalisation of this law is that 20% of the causes are responsible for 80% of the consequences, which, put in another way, can be perceived as saying that 20% of the employees are responsible for 80% of the information flowing through communication channels and influencing opinions.

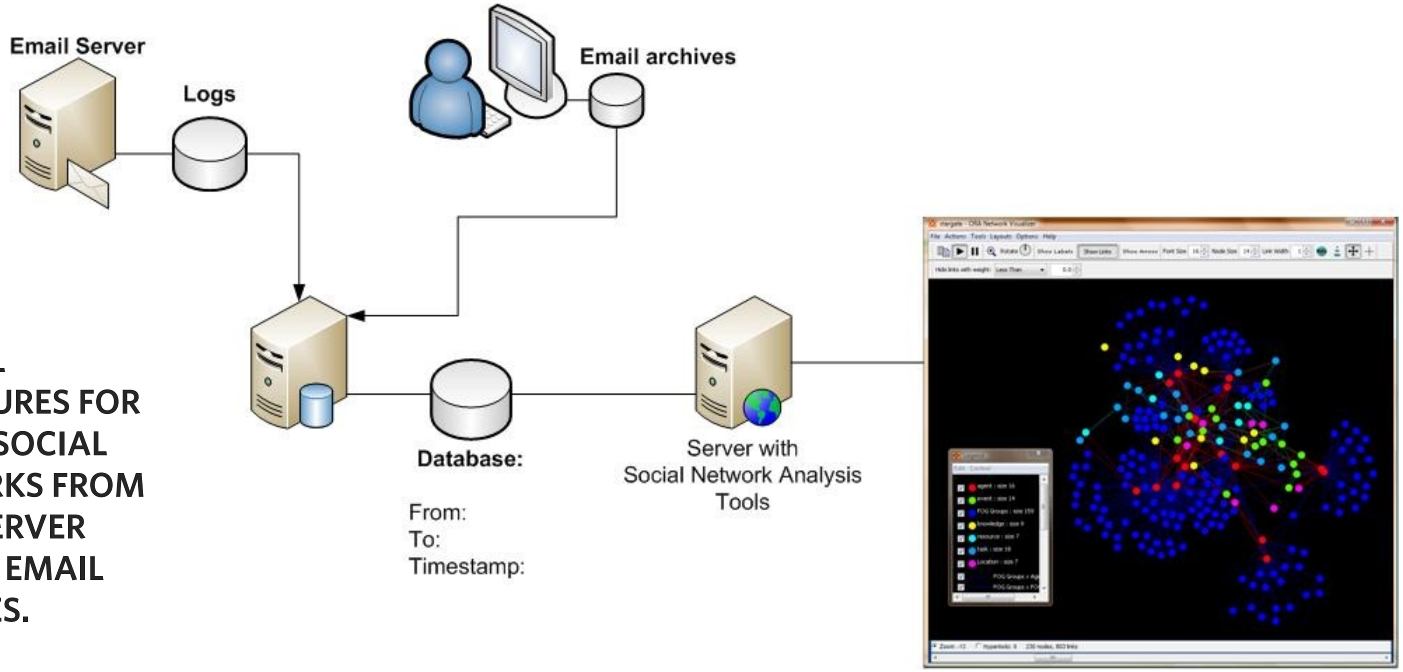
SOCIAL NETWORK ANALYSIS

One methodology used to unveil these 'opinion leaders' and 'bridges' is to conduct a Social Network Analysis. There are several methods to conduct this but one method that has worked is 'data mining' on either electronic mail logs or directly from e-mail messages between employees within the same organisation. It is important to stress that this action would have to be known to the employees in question so that their rights have not been invaded.

The information required to perform this task is already stored on email server logs in the fields "From", "To", and the message's timestamp "Received" and "Sent". This can be used to plot a graphical 'sociogram' where a node in the graph is a person who sent or received an email and the arc linking any two nodes denotes a message sent from one to the other.

A generalisation of the common procedure that researchers follow in order to mine social networks from email logs or email archives are:

a) Identification of communities within the organisation by applying a clustering algorithm.



GENERAL PROCEDURES FOR MINING SOCIAL NETWORKS FROM EMAIL SERVER LOGS OR EMAIL ARCHIVES.

HOME

BEHAVIOURISM AND GROUP COMMUNICATION

SOCIAL NETWORK ANALYSIS

OUTLINING THE CAMPAIGNS

COMMUNICATION CHANNELS

STRATEGY SUMMARY

SOURCES

b) Identification of informal communication roles and informal communication networks.
c) Measurement of socio-metric data.

In order to identify well-connected nodes, the typical measurements involved in an SNA are:

- **Individual connectedness,** which provides the degree of linkage of a particular member. This index could be useful in determining the extent to which a particular member is influenced by the system.
- **Individual integration,** which indicates the degree in which the members of the personal network of an individual are interconnected among each other.
- **System connectedness,** which indicates the degree in which the cliques (a group that ranges from 5 to 25 members in average) of a given social system are interconnected among each other. This index is particularly useful to assess the extent in which innovations are expected to be efficiently diffused within the organisation.

> *“Positive actions are much more likely to affect behavioural changes to security, and this can be targeted by examining the communication channels.”*

OUTLINING THE CAMPAIGNS

Too often, the topic of information security is negative. Coercing individuals to ‘not’ do something is in itself a negative act. Positive actions are much more likely to affect behavioural changes to security, and this can be targeted by examining the communication channels. In the Figure below we see the Innovation-Decision process.

In the Figure on page 7, ‘Knowledge’ includes the Information Security Policy, procedures and guidelines. In a sense this constitutes one Information Security Campaign, namely an Information Security Knowledge Campaign (ISKC). The next stages, from ‘Persuasion’ to ’Implementation’ addresses an allied, but separate issue of persuading individuals to adopt the awareness programme or campaign from the actual imple-

HOME

BEHAVIOURISM AND GROUP COMMUNICATION

SOCIAL NETWORK ANALYSIS

OUTLINING THE CAMPAIGNS

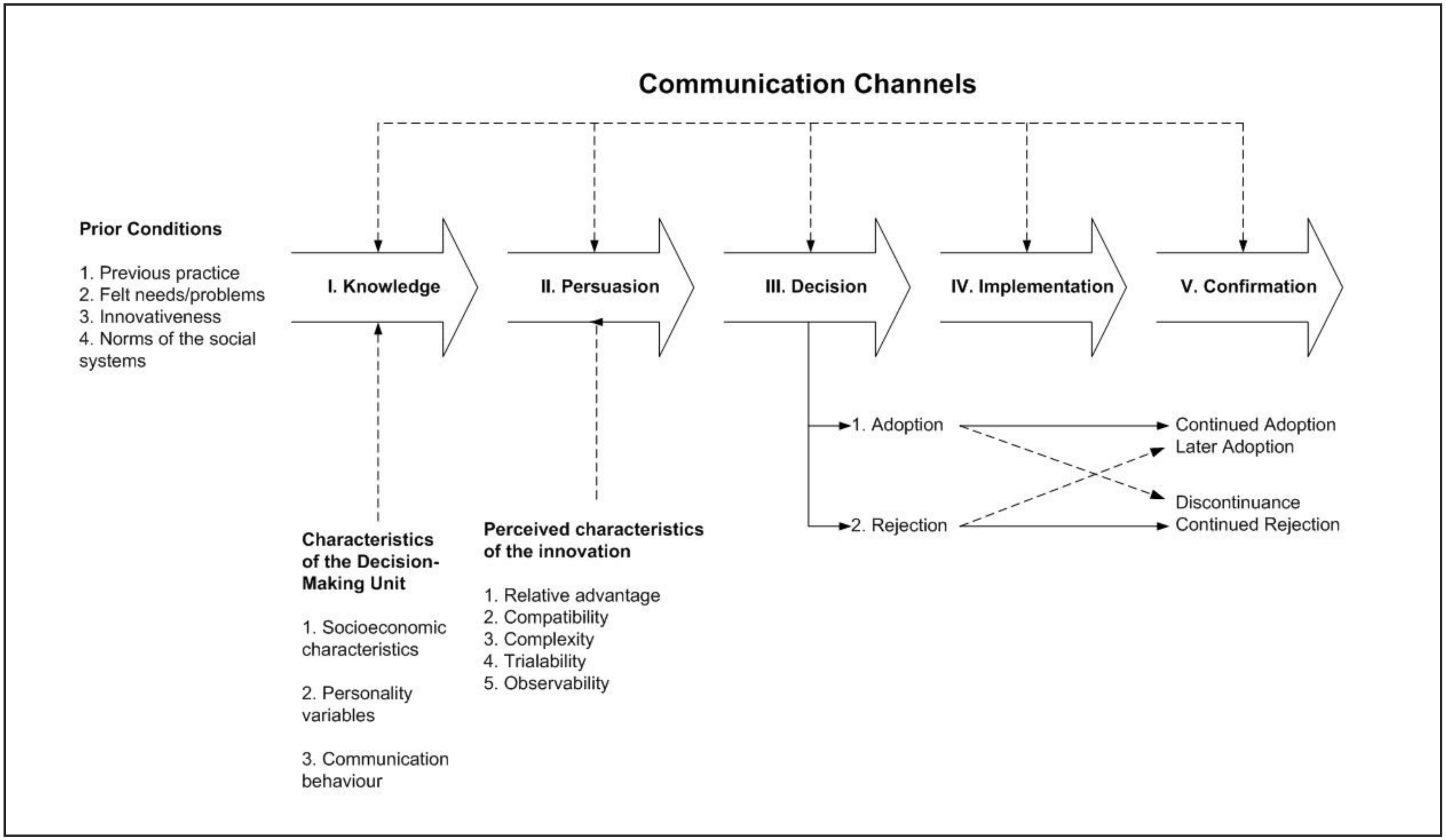
COMMUNICATION CHANNELS

STRATEGY SUMMARY

SOURCES

mentation of the programme. This can be referred to as The Information Security Persuasion Campaign (ISPC). The last stage is 'Confirmation' which is designed to provide further information to employees to help them to support and adopt security behaviour. This can be supported by an Information Security Confirmation Campaign (ISCC).

So, the overall design of this communication channel consists of two broad phases. The first



HOME
BEHAVIOURISM AND GROUP COMMUNICATION
SOCIAL NETWORK ANALYSIS
OUTLINING THE CAMPAIGNS
COMMUNICATION CHANNELS
STRATEGY SUMMARY
SOURCES

(ISKC) includes all tasks of gathering the information, and the second is that of persuasion and adoption.

Normally, information security administrators will be responsible for implementing these campaigns. As part of their task is persuasion, they are sometimes known as ‘change agents’.

The ISKC can be regarded as a communication process between the change agent and employees. This implies that employees should have the opportunity to share their points of view regarding the ISA initiatives promoted by the change agent. The change agent will then have to consider the opinions communicated by employees and adapt the content of the campaign’s messages to reflect a mutual understanding, which eventually would lead to mutual agreement and collective action. However, the extent to which the change agent can reach consensus and achieve mutual understanding and mutual agreement could be questioned, because of the potential high number of employees within the organisation and their dispersion over geographically distant regions. An alternative to this limitation is trying to reach consensus through opinion leaders by applying Pareto’s law; this would mean that if mutual understanding and agreement were reached with opinion leaders, who represent 20% of the employees, then at least 80% of employees would be indirectly involved in such consensus. By trying to seek mutual understanding and mutual agreement with 20% of the employees the result is a far more achievable task than trying to reach such consensus by communicating with the 100% of the employees within the organisation.

The ISPC could be regarded as a communication process between opinion leaders and their followers, and also between employee and employee. This assumption supposes that the opinion leader is actively involved in the diffusion process, by providing further explanations to those followers seeking their support in understanding the security messages, until a mutual understanding and agreement is reached. In addition, further interpersonal network communications are triggered when employees are asked to forward the security message to those who might not know about it. Nonetheless, it would be questionable as to the extent to which opinion leaders are engaged in the ISA initiative and the extent to which employees are expected to talk about the promoted IS issues. The first issue is expected to be sorted by prior conditioning or prior conversations to engage the opinion leaders’ support, the latter issue is addressed by using email content that has proved to engage employees' attention to pass along e-mail. In addition, this latter issue is reinforced by the efforts of 'bridges'—those people who have a connection with many others.

The ISCC could be regarded as a communication process between the change agent and adopters, and between opinion leaders and followers. This campaign represents a form of persuasion, where the change agent and opinion leaders attempt to persuade employees and followers respectively to remain as adopters; hence, the goal of the communication process in the ISCC is to reach mutual understanding and agreement. Table 1 below shows a summary of the proposed strategy to design an ISAP.

Successful communication campaigns have considered the following steps:

1. Conduct formative research.
2. Set SMART goals (acronym for specific, measurable, action-required, realistic, time-delimited goals).
3. Use audience segmentation.
4. Design viral mass media messages.
5. Set the campaign's effectiveness measurement approach.
6. Deliver the ISKC/ISPC/ISCC.

Arguably, one limitation of the proposed approach could be that for every security topic or theme, three different campaigns would be needed, namely the ISKC, ISPC and ISCC, causing additional administration efforts. Nonetheless, the effectiveness of such a strategy may be a compensating factor. Another apparent limitation of this approach is that as three different campaigns need to be conducted, more resources would be needed. This is not necessarily true; since the campaigns are managed from a 20/80 perspective (Pareto's law) where fewer resources are expected to be needed in each delivery. Although this is a debatable point, the hypothesis is that this strategy would consume the same amount of resources provisioned for a traditional ISAP, but with more effective results.

THE COMMUNICATION CHANNELS

It is important to make an annotation regarding the types of communication channels needed for delivery, or, in a more accurate form, the security messages. Two particular types of communication channels are introduced: local channels and cosmopolitan channels. These are the types of channels intended to be used throughout the ISAP. It is important to distinguish between these two types of communication channels in order to determine which is needed to spread a determined piece of information as fast as possible and which is needed for persuasion. For instance, mass communication media such as radio or television are regarded as cosmopolitan communication channels. The cosmopolitan communication channels are more suitable for reaching massive audiences than for persuasion, whereas local channels (inter-personal channels) are more suitable for persuasion than for reaching massive audiences. This means that cosmopolitan communication channels are better for conducting awareness campaigns, whereas local channels are more suitable for launching behavioural change campaigns. For example, a mass communication channel would be used by the change agent to provide knowledge or awareness regarding the compliance requirements of the ISP within the organisation. Then, in order to promote a behavioural change, the opinion leaders' interpersonal channels (which includes face-to-face communication) would be used to deliver specific security guidelines and exert influence towards a positive attitude regarding IS issues.

The columns in TABLE 1 (page 11) are indexed by each phase that takes place when the campaign is targeted to individuals: knowledge, persuasion, decision, implementation and confirmation. The Knowledge Stage is associated with the ISKC (which represent the initial conditioning campaign), the Persuasion Stage is associated with the ISPC (which represent the behavioural change campaign) and the Confirmation Stage is associated with the ISCC (which represent the point of delivery campaign and branding campaign). Similarly each type of communication channels is associated with its corresponding campaign at the corresponding stage.

For the ISKC, which takes place in the first stage, mass-cosmopolitan and inter-personal-communication channels are used to spread as fast as possible the security messages and attempt an initial conditioning towards the acceptance of the security message through the participation of the informal communication roles involved in this stage; namely, bridges and liaisons. When the campaign is launched, the communication process takes place, where the main goal is first to gain a mutual understanding between the change agent and employees and among employees, and then gain knowledge of the campaign being "marketed". For the campaign of this stage, two types of segments are identified: one is comprised of those employees identified as bridges and/or liaisons and the sec-

(Continued on page 12)

TABLE 1

SUMMARY OF THE STRATEGY TO LEAD EMPLOYEES THROUGH THE CAMPAIGN PROCESS

	Campaign Process			
	KNOWLEDGE	**PERSUASION**	**DECISION/ IMPLEMENTATION**	**CONFIRMATION**
Proposed Campaigns	ISKC	ISPC	Indirectly by ISKC and ISPC	ISCC
Marketing Conditioning Principles	**PHASE I:** Initial Conditioning Campaign	**PHASE II:** Behavioural Change Campaign		**PHASE III:** Point of Delivery Campaign and **PHASE IV:** Branding Campaign
Communication channels	Inter-personal-local and mass-cosmopolitan communication channels	Inter-personal-local communication channels		Mass-cosmopolitan and Interpersonal/local communication channels
Informal communication roles	Bridges, Liaisons	Opinion Leaders		Opinion Leaders
Participants in the campaign	Change Agent-Bridges/ Liaisons, and employees-employees	Opinion Leaders-Followers and Employees-Employees		Change Agent-Adopters, Opinion Leaders-Followers and Employees-Employees
Campaign goals	Mutual Understanding Knowledge/Awareness	Mutual Understanding and Mutual Agreement	Induced Collective Action	Mutual Understanding and Mutual Agreement
Segments	2 segments, bridges/ liaisons and IS concerns	2 segments, Opinion leaders and IS concerns.		1 segment (100% of members)
Delivery method	20/80	20/80		20/80
Perceived characteristics	Relative advantage	Compatibility complexity		Relative advantage and compatibility, complexity

HOME

BEHAVIOURISM AND GROUP COMMUNICATION

SOCIAL NETWORK ANALYSIS

OUTLINING THE CAMPAIGNS

COMMUNICATION CHANNELS

STRATEGY SUMMARY

SOURCES

(Continued from page 10)

ond is a group composed of different segments grouped according to their particular security concerns. The delivery method is referred to as the 20/80 campaign delivery mode, which represents an alternative method that copes with the acceptance of a changing environment.

It shall be noted that the decision and implementation stages are not directly influenced with a particular campaign. They are indirectly influenced with the preceding campaigns in order to provide employees with the opportunity to cope with the required security behavioural change in a self-paced manner to avoid any “compulsory impression” which would significantly affect the employees’ attitude towards IS issues.

Finally, a 20/80 delivery mode is proposed. This delivery mode involves sending in advance an “informal” security message to those employees identified as bridges, liaisons and opinion leaders and then launching the formal IS campaign targeting all employees to reinforce the message. This campaign delivery mode represents an alternative method that copes with the acceptance of IS issues in a changing environment. ■

ABOUT THE AUTHORS

Carlos Orozco Corona has been working in information security field for seven years. He currently works at FIRA, Banco de Mexico, as an Information Security Specialist. His main interests in the information security field are: Cryptography, Network and Computer Security and particularly the application of Social Network Analysis in the Information Security arena.

John Austen is a consultant lecturer in information security at Royal Holloway, University of London, after a distinguished career as head of the Computer Crime Unit of New Scotland Yard. He teaches the courses in Computer Crime and Digital Forensics on the M.Sc. in Information Security at Royal Holloway.

HOME

BEHAVIOURISM AND GROUP COMMUNICATION

SOCIAL NETWORK ANALYSIS

OUTLINING THE CAMPAIGNS

COMMUNICATION CHANNELS

STRATEGY SUMMARY

SOURCES

SOURCES:

[1] http://news.zdnet.co.uk/itmanagement/0,1000000308,2129738,00.htm

[2] http://vil.nai.com/vil/content/v_100454.htm

[3] The full MSc project report illustrates an exploit bypassing certain restrictions.