Maximising the Effectiveness of Information Security Awareness

This thesis offers a fresh look at information security awareness using research from marketing and psychology.

By **Geordie Stewart** and **John Austen**

Royal Holloway
University of London

SearchSecurity.co.UK

HOME

KEY POINTS

PSYCHOLOGY

MARKETING

CONCLUSION

MEASURING EFFECTS

KEY POINTS

- Claims are made about the value of promoting information security awareness with little evidence to suggest that current methods are effective
- There is evidence that the link between "awareness" and a change of behaviour is weak and heavily dependent on other factors
- The value of information security awareness needs to be measured by changes in behaviour which have positive outcomes for information security
- Research in psychology shows that an over-reliance on fear sanctions can be counterproductive in risk communications
- A "mental models" approach, mapping existing audience beliefs and attitudes, can significantly improve the success of risk communications
- Traditional information security awareness campaigns fit the profile of "mass marketing" which normally has a very low "success" rate
- "Direct marketing" is an ideal methodology for organisations seeking to influence their information systems users and employs targeted communications for maximum effect

INTRODUCTION

Over the last twenty years, technical controls for information security have advanced and matured considerably. However, despite these technical advances, information security breaches still occur on a regular basis. It appears that technical security controls have evolved faster than management controls. Despite efforts at promoting information security awareness there is evidence that human behaviour remains a significant vulnerability in any information security system.

Awareness campaigns are designed and implemented often at great cost to organisations - yet are we more secure as a result? Evidence suggests that common industry methods and practices used to promote information security awareness are ineffective. Not only is the promotion of awareness a costly and difficult venture, but the link between awareness and change in behaviour has been shown to be weak.

At a personal level we are bombarded on a daily basis to give up smoking, stop speeding and lose weight—if these messages are routinely ignored why should information security messages be any different?

If the goal of security awareness is to influence

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS

human behaviour then disciplines specialising in the study of influencing human behaviour such as psychology and marketing offer an opportunity to review and improve the effectiveness of information security awareness techniques.

PSYCHOLOGY

Psychology is an established discipline of academic research dealing with human behaviour and motivation. It offers the opportunity for increased understanding and prediction of human actions through the appreciation of the cognitive functions underlying the behaviour. This increased understanding could be invaluable to information security professionals when attempting to predict the outcome of communication efforts directed at information security awareness.

Operant Conditioning: The study of "operant conditioning" is the study of human behaviour as a function of punishments and rewards. "Positive punishment" is the addition of undesirable stimulus which serves to discourage any associated behaviours while "positive reinforcement" is the addition of desirable stimulus and serves to increase the frequency or magnitude of associated behaviours.

When an organisation has problems with behaviour impacting information security, it is important to recognise the implications of operant conditioning, which suggests that all behaviour exists because it is or has been rewarded in some way:

> *"When organisations face problems with costs, quality, productivity and attendance, these problems often stem from ineffective patterns of behaviour that the organisation is unwittingly encouraging. To prevent and stop these problems, a behavioural approach to managing people is often the most effective."*
>
> —Peter Makin and Charles Cox:
> Changing Behaviour at Work

Makin and Cox note that when seeking to discourage unwanted behaviour the "natural reaction" is to resort to the traditional stick approach – to punish behaviour which is considered non-compliant rather than rewarding patterns of compliant behaviour. Punishment often consists of pressure and cajoling from management. This approach, which is often used to promote compliance with security management controls, may not always be the most effective motivator in the operant conditioning equation. Recent examples from the field of organisational management have shown that rewards can be more effective tools depending on the situation. The critical factors to consider when deciding the approach to use are the timing of the response and asymmetry that exists between reward and punishment.

The timing of the response effectively refers to the delay between the behaviour and its response. A change in behaviour under this circumstance depends on the subject perceiving the link between the action and the response. The longer the time period between these two events, the weaker the influence on the subject. In an information security context it is important to consider if there is a difference between punishment and reward in how quickly the consequence can be delivered.

The reward/punishment paradox refers to the fact that while behaviours can be effectively encouraged through occasional rewards, punishment must be consistent in order to have the same impact, unless the punishment is significantly severe in some way. In an information security context it is important to consider that in some situations it may not be possible to implement a punishment for each example of the behaviour. For instance it may not be possible to reliably detect the occurrence of the behaviour. If punishments cannot be reliably delivered for each example of the behaviour it is likely that an occasional reward of the desired behaviour state would be more influential. It should also be noted that an important potential unintended consequence of relying on punishments is that people may have an incentive not to report an information security breach.

Fear Response: It is common for information security awareness messages to appeal to fear as a motivator. While it might be expected that the degree of influence that a fear has is simply a function of its severity it appears the results are more complicated. The “Boomerang Effect” has been defined by Kim Witte as an explanation for why an individual’s response to the severity of fear eventually has a declining impact.

Where the individual perceives that danger and their own ability to manage the danger is high, they are likely to take steps to control the risk. However, if the danger is high but the individual perceives a low ability to manage the danger, the individual is likely to develop a “Cognitive Dissonance”. This is when a contradiction exists between two cognitions or thoughts. This could include a contradiction between attitudes and

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS

actual behaviour. Psychologist Stephen Pinker states that cognitive dissonance is an uncomfortable state for the individual. The surprising result is that instead of changing behaviour to remove the conflict the individual is more likely to "invent a new opinion" to resolve the conflict. This goes some way to explain why so many people continue to take risks even when the awareness of the danger improved. Rather than change their behaviour they may have adopted a coping mechanism.

Mapping existing audience beliefs and attitudes is a critical prerequisite to understanding how an audience will process and interpret risk communications.

Coping mechanisms might include denial or other rationalisations such as "it will never happen to me". A case study is presented in the full thesis for an organisation that has used rewards to motivate compliance behaviour instead of relying on fear sanctions. Since the perception of fear and perceived control efficacy is an individual property it makes it difficult for an organisation to find an optimum level of fear appeal where sufficient motivation is gained for some subjects without creating risk apathy in others. This suggests that organisations should either carefully target fear appeals to segmented audiences or use rewards instead to avoid the boomerang effect altogether.

Excessive fear is also associated with a decline in cognitive effectiveness. The implication is that it might be possible to scare users with information security threats and risks to the extent that they start to make mistakes.

Mental Models: Research into relevant psychology principles shows that the mental models approach advocated by risk communications expert M. Granger Morgan is of significant benefit. Mapping existing audience beliefs and attitudes is a critical prerequisite to understanding how an audience will process and interpret risk communications. Risk communications will likely have unintended consequences if audiences have

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS

significantly different understandings about any referenced concepts such as "risks" and "threats". The full thesis contains the results of a mental models study completed in a large UK organisation. Responses were invited from three separate teams: HR, Information Security and Finance. Questions tested beliefs such as "A risk is the same thing as a threat" and attitudes such as "I should consider someone's motivations before reporting them for suspected breaches of information security policy".

Not only were interpretations of key concepts found to be inconsistent between teams, but the results were also internally inconsistent as members of the same teams had a significant range of interpretations. It is clear that any information security awareness campaign employed in this environment would need to reconfirm basic definitions before proceeding. The concept of risk perception is exposed as a uniquely personal interpretation that organisations need to consider before embarking on any communications exercise.

> *The concept of risk perception is exposed as a uniquely personal interpretation that organisations need to consider before embarking on any communications exercise.*

Heuristics: Humans appear to be broadly logical creatures but some systematic failures have been identified in human risk perception. Heuristics are mental shortcuts that are a consequence of the need to make decisions in a short period of time. The extent of human rationality can be measured in a laboratory setting, but this does not represent real world decision making which is likely to take place with distractions and time pressures. As a result of the need to make decisions in a relatively short period of time it appears that humans have evolved cognitive shortcuts for responding to risks. Generally, we focus on risks that are new, unfamiliar, controlled by others and ill-defined in some way (such as radiation leaks and hackers). Risks which are familiar and can be

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS

controlled by the individual in some way are perceived as less risky (such as our own driving or remembering to backup your data).

While these mental shortcuts can lead to bias and behaviour which appears illogical, this behaviour is also predictable to some degree. Information security professionals need to measure and anticipate the cognitive biases present in their audiences and adjust their information security awareness messages accordingly.

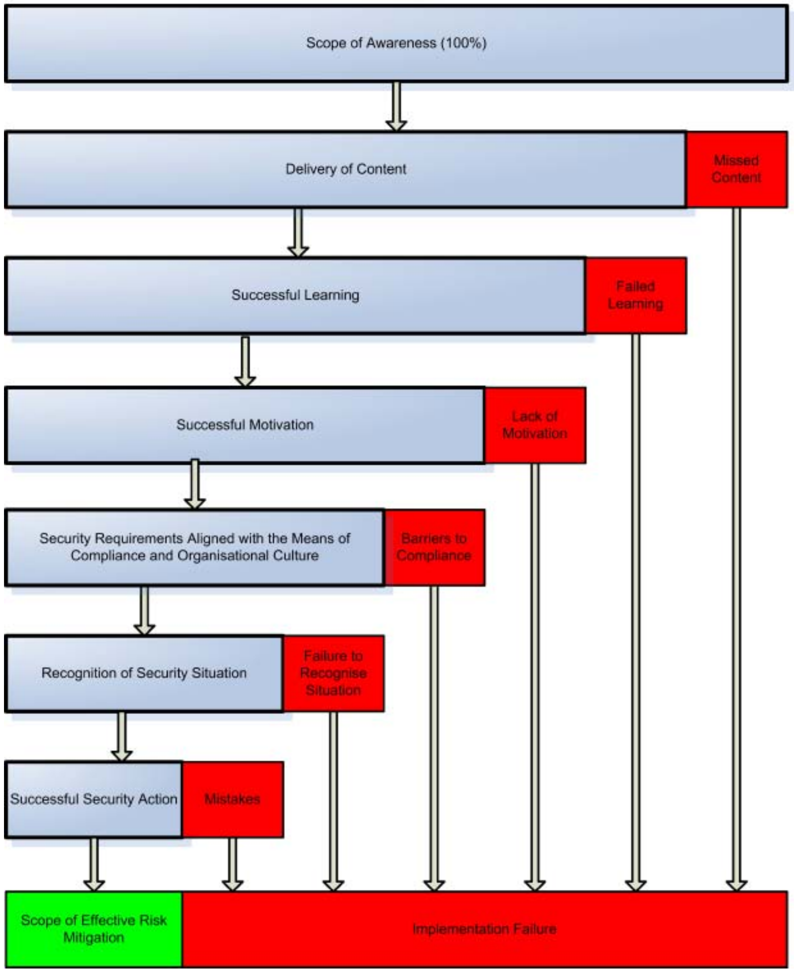
Predicting Awareness Effectiveness: The following model has been created to show the points of failure that could prevent the success of an information security awareness message.

MARKETING

Traditionally, marketing is thought of as an activity which is done for profit. However, it is not always the case that marketing is done to create a demand for a product or service. The closest marketing example for information security awareness would probably be government marketing cam-

FIGURE 1

STEPS INVOLVED IN REALISING BENEFITS FROM INFORMATION SECURITY AWARENESS


Scope of Awareness (100%)
Delivery of Content
Missed Content
Successful Learning
Failed Learning
Successful Motivation
Lack of Motivation
Security Requirements Aligned with the Means of Compliance and Organisational Culture
Barriers to Compliance
Recognition of Security Situation
Failure to Recognise Situation
Successful Security Action
Mistakes
Scope of Effective Risk Mitigation
Implementation Failure

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS

paigns such as "Think! Road Safety", an initiative that seeks to influence the behaviour of drivers and other road users. The similarities to information security awareness are:

1. Profit is not the primary objective although there may be a significant shared economic benefit from reducing road accidents

2. Awareness of risk is one of the key components which the campaign seeks to communicate

Traditional information security awareness campaigns often use a mass marketing format. Generic messages are sent to an audience via screen savers, posters and mouse mats which promote awareness of information security but often with very little in the way of a measurable behaviour change. The problem is that a change in awareness does not necessarily result in a change of behaviour.

Direct Marketing: Direct marketing is an alternative marketing methodology that focuses on individuals and has two important distinctions from mass marketing. Firstly, communications take place in the context of an ongoing discussion where both parties can learn about the other and communications become progressively more effective based on preferences expressed by both parties. Secondly, the defining feature of direct marketing is the expected result – a call to action of some sort on behalf of the recipient. Rather than dealing with concepts as abstract as brand awareness, direct marketing has an empirical outcome expected of each set of interactions. The outcome could be to change a password, visit a web site, or to book security training. Attributing the responses received allows methods to be refined and a return on investment (ROI) to be calculated. So typically a mass marketing approach is one size fits all, often with little in the way of immediate empirical results, while direct marketing is tailored to the individual in some way and expects an immediate and measurable outcome.

Organisations can leverage the information they hold about their information system users for a shared benefit within the restrictions of the Data Protection Act. Consider that there is usually already a relationship between the organisation and a target audience, who could exist as employees or customers of its information system, which can be exploited by direct marketing. Most organisations would already have a significant database of information about their poten-

HOME

KEY POINTS

PSYCHOLOGY

MARKETING

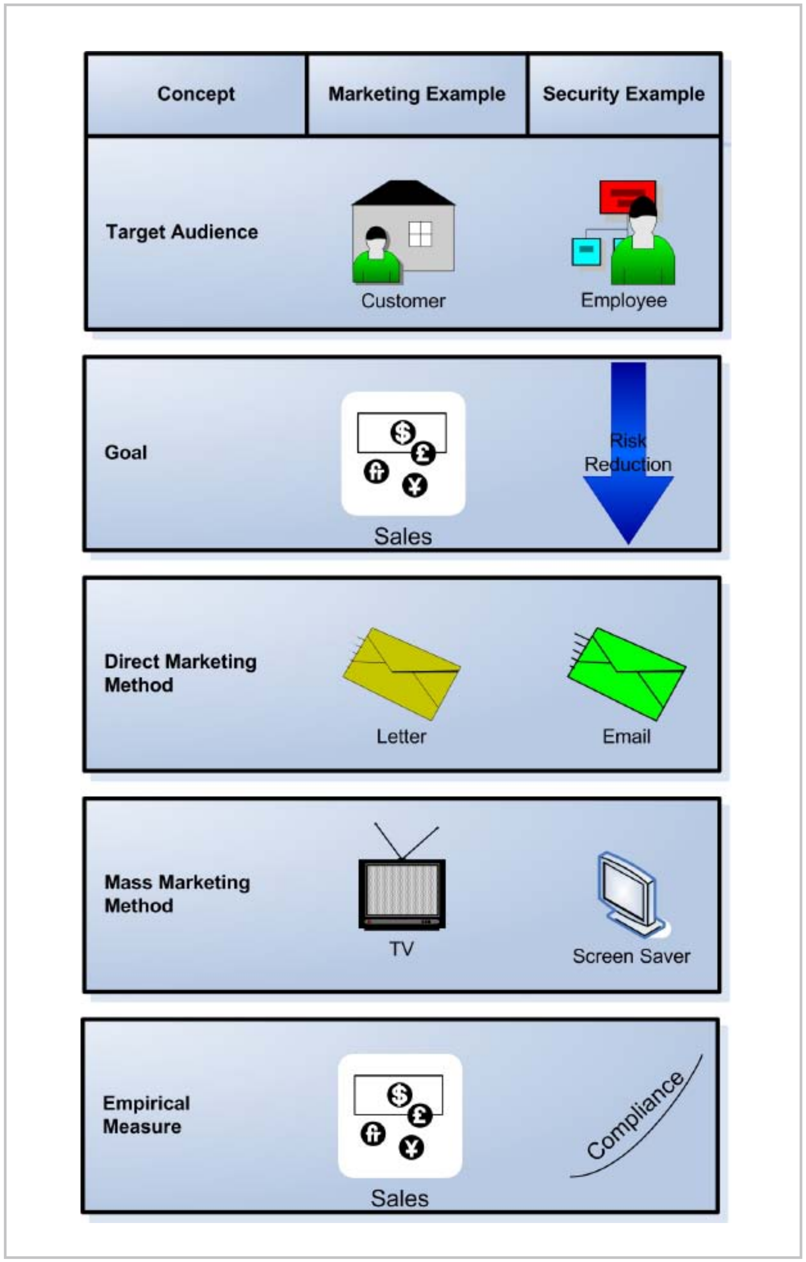
CONCLUSION

MEASURING EFFECTS

tial audience which would show many preferences and attributes useful for designing communications. For employees the company is likely to hold job title, age, sex, address, department, length of employment, and how many times they have called IT for support. These are all useful attributes to know when attempting to understand the perspectives and likely responses of an audience when exposed to security communications.

Direct marketing maximises the effectiveness of communications by focusing on audience research, measuring existing attitudes and finding quantifiable metrics as essential tools to maximise results. How many organisations embark on awareness activities without considering any of these factors? If information security awareness really is as important as so many information security practitioners make it out to be, then is it not worth doing effectively? Taking a direct marketing approach to information security awareness could hold the answer to the problem of attaining and demonstrating effective communication.

The example at right illustrates the key differences between marketing activities undertaken for profit and marketing activities used in an information security context.



Concept	Marketing Example	Security Example
Target Audience	Customer	Employee
Goal	Sales	Risk Reduction
Direct Marketing Method	Letter	Email
Mass Marketing Method	TV	Screen Saver
Empirical Measure	Sales	Compliance

HOME

KEY POINTS

PSYCHOLOGY

MARKETING

CONCLUSION

MEASURING EFFECTS

CONCLUSION

A recurring theme in the review of information security awareness effectiveness is a lack of metrics to demonstrate the impact of information security awareness. Information security practitioners need to find ways of measuring results in the form of quantifiable behaviours. Measuring attitudes and beliefs through the use of surveys has been found to have a poor correlation with actual behaviour.

This lack of metrics causes problems with obtaining business support for awareness programmes and creates difficulties for us in improving our awareness techniques.

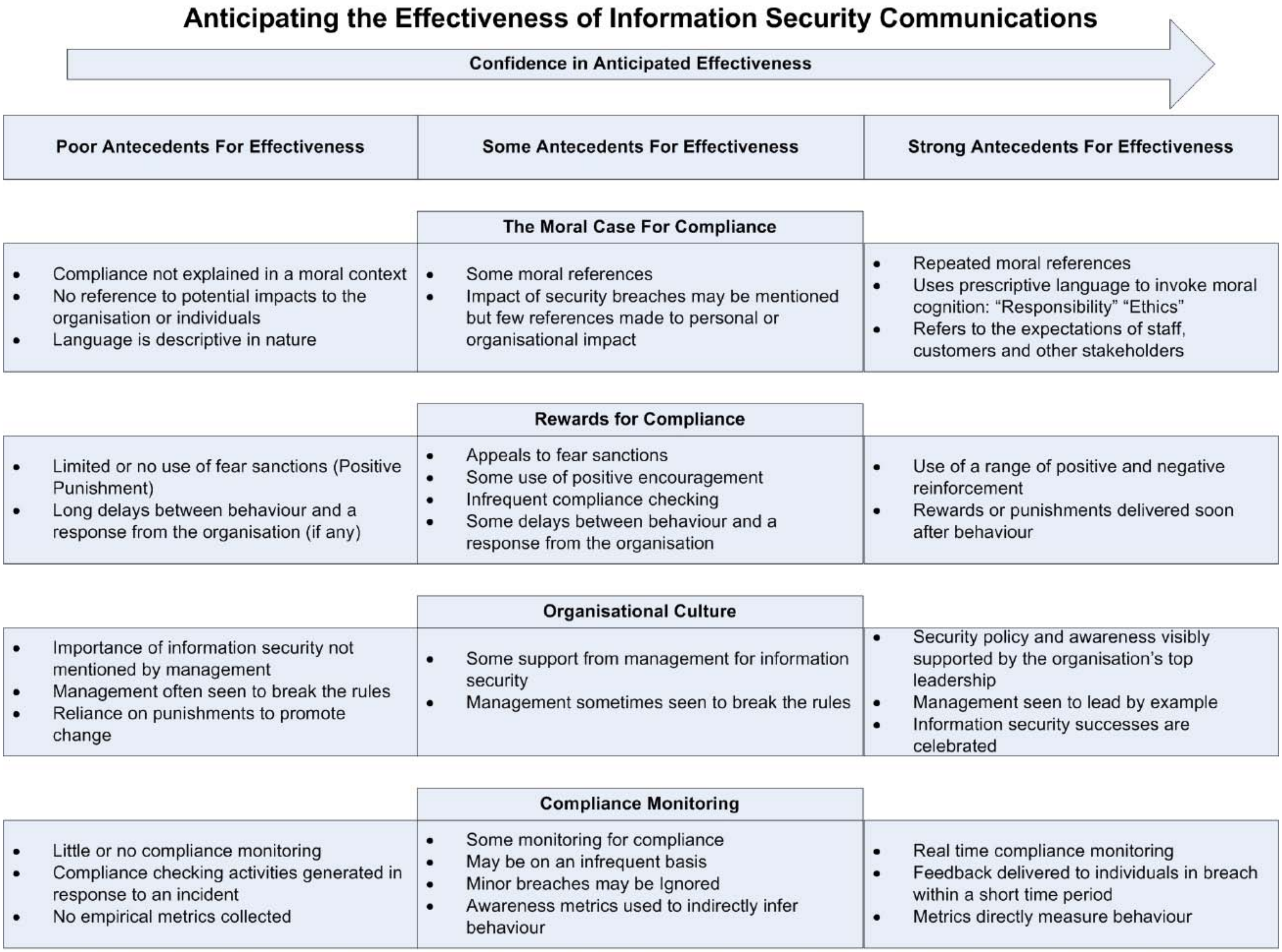
This lack of metrics not only causes problems with obtaining business support for information security awareness activities, but has also contributed to a difficulty in improving information security awareness techniques. The bedrock of the Plan, Do, Check, Act management cycle is reliable metrics. If there are no reliable ways available to an organisation to demonstrate the effectiveness of a particular technique, how can improvements be made by identifying that one technique was more effective than another? Although potential ways of improving information security awareness using psychology and marketing principles have been identified, the benefits will be difficult to demonstrate because of the lack of metrics.

Information security professionals have contributed to this lack of metrics but they are also part of the solution. We need to move beyond glib statements about the "criticality" of awareness and focus on making a business case for awareness activities. All behaviour has a consequence and some consequences are easier to measure than others. Information security professionals need to find ways of measuring these consequences to infer the effectiveness of communication techniques.

The reference model shown on pages 11 and 12 has been created to show designers and implementers of information security awareness pro-

(Continued on page 13)

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS

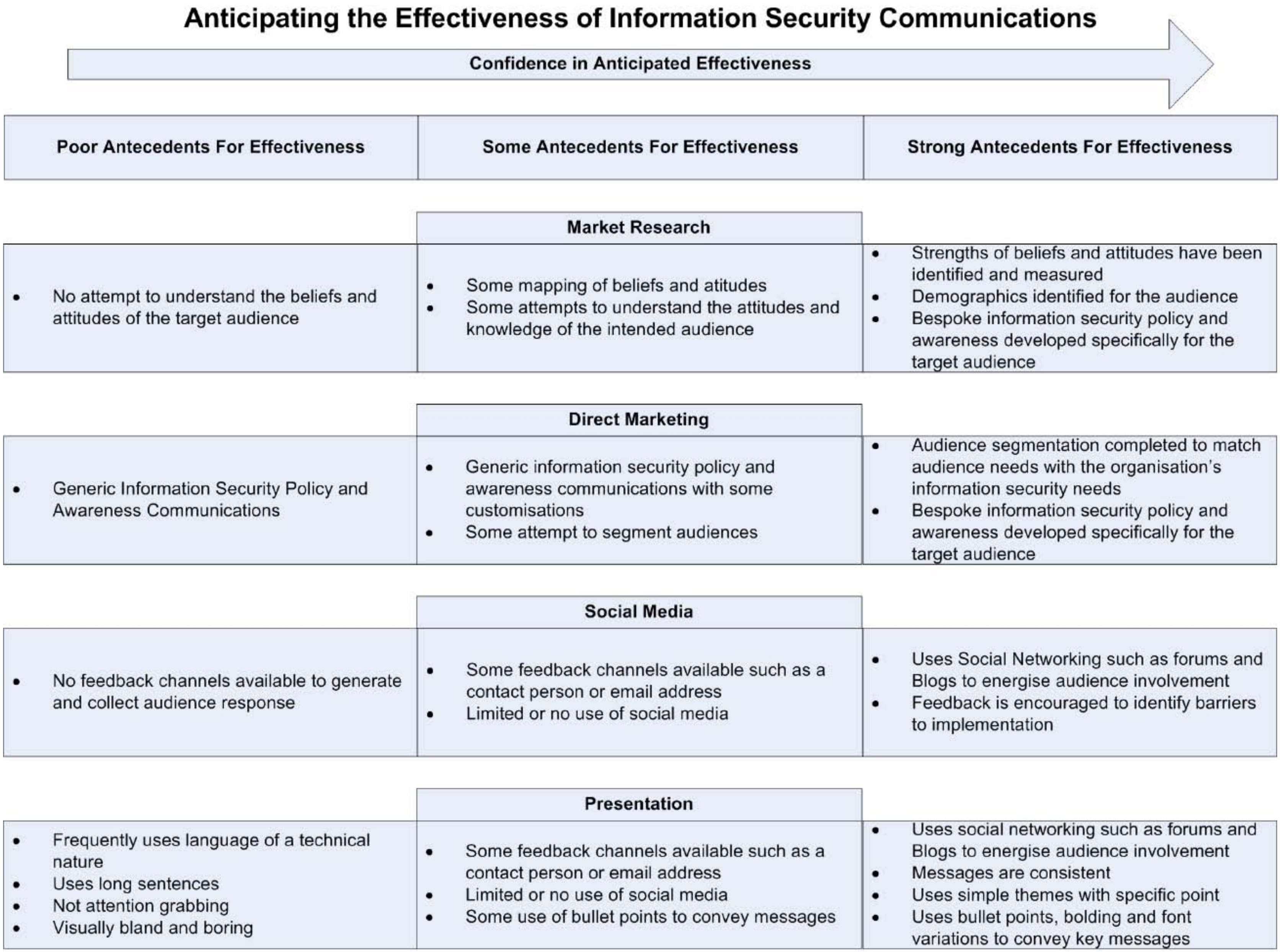


Anticipating the Effectiveness of Information Security Communications

Confidence in Anticipated Effectiveness

Poor Antecedents For Effectiveness	Some Antecedents For Effectiveness	Strong Antecedents For Effectiveness
	The Moral Case For Compliance	
• Compliance not explained in a moral context • No reference to potential impacts to the organisation or individuals • Language is descriptive in nature	• Some moral references • Impact of security breaches may be mentioned but few references made to personal or organisational impact	• Repeated moral references • Uses prescriptive language to invoke moral cognition: “Responsibility” “Ethics” • Refers to the expectations of staff, customers and other stakeholders
	Rewards for Compliance	
• Limited or no use of fear sanctions (Positive Punishment) • Long delays between behaviour and a response from the organisation (if any)	• Appeals to fear sanctions • Some use of positive encouragement • Infrequent compliance checking • Some delays between behaviour and a response from the organisation	• Use of a range of positive and negative reinforcement • Rewards or punishments delivered soon after behaviour
	Organisational Culture	
• Importance of information security not mentioned by management • Management often seen to break the rules • Reliance on punishments to promote change	• Some support from management for information security • Management sometimes seen to break the rules	• Security policy and awareness visibly supported by the organisation’s top leadership • Management seen to lead by example • Information security successes are celebrated
	Compliance Monitoring	
• Little or no compliance monitoring • Compliance checking activities generated in response to an incident • No empirical metrics collected	• Some monitoring for compliance • May be on an infrequent basis • Minor breaches may be Ignored • Awareness metrics used to indirectly infer behaviour	• Real time compliance monitoring • Feedback delivered to individuals in breach within a short time period • Metrics directly measure behaviour

HOME
KEY POINTS
PSYCHOLOGY
MARKETING
CONCLUSION
MEASURING EFFECTS



Anticipating the Effectiveness of Information Security Communications

Confidence in Anticipated Effectiveness

Poor Antecedents For Effectiveness	Some Antecedents For Effectiveness	Strong Antecedents For Effectiveness
	Market Research	
• No attempt to understand the beliefs and attitudes of the target audience	• Some mapping of beliefs and atitudes • Some attempts to understand the attitudes and knowledge of the intended audience	• Strengths of beliefs and attitudes have been identified and measured • Demographics identified for the audience • Bespoke information security policy and awareness developed specifically for the target audience
	Direct Marketing	
• Generic Information Security Policy and Awareness Communications	• Generic information security policy and awareness communications with some customisations • Some attempt to segment audiences	• Audience segmentation completed to match audience needs with the organisation's information security needs • Bespoke information security policy and awareness developed specifically for the target audience
	Social Media	
• No feedback channels available to generate and collect audience response	• Some feedback channels available such as a contact person or email address • Limited or no use of social media	• Uses Social Networking such as forums and Blogs to energise audience involvement • Feedback is encouraged to identify barriers to implementation
	Presentation	
• Frequently uses language of a technical nature • Uses long sentences • Not attention grabbing • Visually bland and boring	• Some feedback channels available such as a contact person or email address • Limited or no use of social media • Some use of bullet points to convey messages	• Uses social networking such as forums and Blogs to energise audience involvement • Messages are consistent • Uses simple themes with specific point • Uses bullet points, bolding and font variations to convey key messages

(Continued from page 10)

grammes how to align with psychology and marketing principles and serves as a snapshot to evaluate the likely effectiveness of a given campaign. This includes principles such as risk perception, learning and motivation for the modification of behaviour. ■

ABOUT THE AUTHORS

Geordie Stewart is an IT Security Consultant working for Network Rail. He is a New Zealander who has lived in London for 5 years and his security experience includes finance, retail banking, telecommunications and insurance. His technical qualifications include Microsoft, Checkpoint, Citrix and ISS. Geordie's professional interest is in understanding user behaviour in an information security context.

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

KEY POINTS

PSYCHOLOGY

MARKETING

CONCLUSION

MEASURING EFFECTS