Combatting Phishing: A Holistic Human Approach

Edwin D. Frauenstein[1] and Rossouw von Solms[2]
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
edwin.frauenstein@gmail.com[1], rossouw.vonsolms@nmmu.ac.za[2]

***Abstract*—Phishing continues to remain a lucrative market for cyber criminals, mostly because of the vulnerable human element. Through emails and spoofed-websites, phishers exploit almost any opportunity using major events, considerable financial awards, fake warnings and the trusted reputation of established organizations, as a basis to gain their victims' trust. For many years, humans have often been referred to as the 'weakest link' towards protecting information. To gain their victims' trust, phishers continue to use sophisticated looking emails and spoofed websites to trick them, and rely on their victims' lack of knowledge, lax security behavior and organizations' inadequate security measures towards protecting itself and their clients. As such, phishing security controls and vulnerabilities can arguably be classified into three main elements namely human factors (H), organizational aspects (O) and technological controls (T). All three of these elements have the common feature of human involvement and as such, security gaps are inevitable. Each element also functions as both security control and security vulnerability. A holistic framework towards combatting phishing is required whereby the human feature in all three of these elements is enhanced by means of a security education, training and awareness programme. This paper discusses the educational factors required to form part of a holistic framework, addressing the HOT elements as well as the relationships between these elements towards combatting phishing. The development of this framework uses the principles of design science to ensure that it is developed with rigor. Furthermore, this paper reports on the verification of the framework.**

Keywords—phishing; social engineering; human factors; organizational aspects; technological controls; security education training and awareness; agency theory; technology acceptance model; COBIT

I. Background of Phishing and HOT Relationships

A cyber security study conducted by Deloitte revealed that chief information security officers (CISOs) are of the opinion that phishing and pharming currently pose the main cyber security threat to their respective organizations [1]. Phishing is a concern, for both organizations and consumers, because of phishers' ability to skilfully mimic legitimate organizations in the technical design of their emails and websites. Phishing costs organizations and their clients billions of dollars in lost revenue every year. The traditional approach of phishers targeting solely financial institutions in emails has transformed. Phishers take advantage of popular events and adapt to certain leading trends, thereby creating more confusion for consumers to distinguish legitimate emails from phishing. For example, phishers used a popular game known as 'Warlords of Draenor' to scam gamers into believing that they won a free copy of the game [2]. Instead, the phishers stole their login credentials. Furthermore, phishers are increasingly using social networks and phone text messages to reach a larger audience. Recently, phishers spoofed a Facebook webpage with the poster of Arvind Kejriwal, the Indian leader of the Aam Aadmi Party, in order to acquire Indian Facebook users login credentials [3].

Phishing attacks are increasing at a rapid rate. South Africa is the second most targeted country globally with costs amounting to approximately $320 million in 2013 only, and account for 5% of the total volume of all global phishing attacks [4]. A study conducted by the Anti-Phishing Work Group (APWG), revealed that there were at least 115,565 unique phishing attacks worldwide, nearly a 60% increase over the first half of 2013 – setting record levels [5]. A large proportion of the phishing attacks were directed at China. Nearly one-third of all attacks, 32.9%, were directed at banks and another 17.5% targeted money-transfer services. PayPal was the most-targeted institution with 24,580 attacks [5]. Half of the targets were attacked at least three times during the six-month period. Another concern is amateur phishers can use 'phishing kits' (easily found online) which contain templates for popular targets. Furthermore, organizations can be breached for many years unsuspectingly. The longest period an attacker was present before being detected in 2013 was six years and three months [6]. With the widespread use of smartphones and tablet devices at home and in the workplace, users could unsuspectingly compromise both personal and organizational information stored on these devices.

Phishing is effective because victims are deceived into believing the emails and spoofed websites originate from a trusted source. However, if users are effectively educated in the technical features active in phishing, it would be possible for them to be able to identify it as phishing. This would require that users must be educated in the technological tools such as their web browser, anti-virus programs, email client and their warning alerts and so on. Also users must receive education to recognize certain psychological triggers (i.e. social engineering techniques) that are being used by phishers. This is often referred to the 'bait' which is one of the main causes for users being led into believing the warnings and/or the substantial rewards being offered is real.

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

Phishing threat agents exploit a number of elements namely; the human factors (H), organizational aspects (O) and technological controls (T) [7]. Ideally, if all elements could be working synchronously instead of independently, a holistic framework, consisting of the HOT elements, could be formed. In each of these elements, human involvement is common. As such, educating users is imperative in order to address phishing threats satisfactorily. Reference [8] used real-world phishing scenarios to establish three main sets of relationships that exist in typical phishing attacks, namely; human and technology (HT), human and organization (HO) and, finally, organization and technology (OT). Furthermore, each of these relationships is related to various theories and best practices. The Technology Acceptance Model (TAM) is related to the HT relationship, because the TAM suggests that when users are presented with a new technology, a number of factors influence their decision about how and when they will use that technology. As discussed by Davis [9], these two factors are perceived; ease of use and usefulness. Thus, TAM provides guidance on how the users need to be prepared to effectively utilize the technical phishing countermeasures installed by the organization. Agency theory is related to HO relationship and is concerned with the relationship between the principal (organization) and the agent (employee), who both have opposing goals (e.g. compensation, regulation, leadership) and risk preferences (e.g. whistle blowing, vertical integration, transfer pricing). Agency theory is concerned with resolving two problems namely; the conflicting desires or goals of the principal and agent and the verification of the agent's activities, which is too difficult or expensive for the principal [10]. Policies and procedures are typically used to define the relationship between the principal and the agent. Therefore, policies and procedures are commonly found to espouse the behavioral relationship between the organization and its employees, also in the case of phishing. Finally, COBIT is a best practice related to the OT relationship as it concerns aligning IT with the organization's needs. This alignment refers to "applying IT in an appropriate and timely way, in harmony with the business strategies, goals and needs" [11]. Thus, a best practice such as COBIT can effectively be used to ensure that the organizations and its IT goals are properly aligned.

Establishing and addressing these relationships achieved a number of objectives: (1) it established that security gaps exist within each of these relationships; and (2), it provided guidance to help identify components that can be used to strengthen each of these relationships [8]. It emerged that education is inevitably a major role player in each of these as humans and their behavior is actively participating in all. These relationships will be used in this paper to structure the educational components.

As such, the objective of this paper is to identify and discuss the educational components required in each of the HOT relationships to address factors associated with phishing. The rest of the paper is structured as follows: section 2 begins by discussing the problem area of human factors with regard to general information security and how it can be treated. Section 3 describes the educational components needed to address each of the respective relationships. Section 4, discusses the verification of the underlying HOT framework.

II. Treating the Human Factor in Information Security

As discussed earlier, humans have either a direct or an indirect involvement with each of the processes in the relationships. It is imperative that human behaviour is addressed through security awareness, training and education in order to change the ideas and behaviour of users in an organisation [12]. The greatest influences stemming from human factors are the attitudes, behaviour, motivation, commitment, habits and norms of people. Unfortunately, very little is known about why users choose to engage in unsafe security behavior [13]. Humans tend to be curious by nature and thus, it is difficult to predict their actions. According to Lacey [14], changing human behavior is more difficult than changing attitudes. If human behavior could be better understood, then one could suitably address why humans fall victim to phishing emails [15]. Leach [16] states that three key factors are necessary to improve user behavior in information security. These factors are: (1) The behavior demonstrated by senior management and colleagues (2) The user's security common sense and decision-making skills and finally (3) the strength of the user's psychological contract with the company. Coincidentally, these key factors correspond with each of the three relationships of [8]. It is widely recognized that modern day security threats focus mostly on exploiting human behavior and knowledge [17]. In this paper, user attitudes and behaviors are primarily focused on addressing three main objectives relating to the respective relationships, namely: (1) using technological security controls correctly, (2) obeying organizational policies and procedures, and (3) influencing management and employees' commitment and support of information security. These three objectives are discussed in the next section, and can help combat phishing attacks however, this is dependent on both knowledge and cooperation of humans [18].

III. Educational Components Required To Strenghten the HOT Relationships

By creating a holistic framework that considers human, organizational and technological aspects, an organization should be better protected against phishing threat agents. The interrelationship between the human aspects, organizational aspects and technological controls of the HOT framework, is discussed as follows. From an organizational perspective, management has a responsibility to ensure that its information assets are adequately protected from phishing threat agents. To accomplish this, the organization (i.e. management) can use best practices, such as COBIT, to help identify the suitable technological controls needed to protect the organizational information. This can be defined as the OT relationship. Furthermore, the organization must also ensure that adequate policies and procedures are implemented in order to dictate the behavior of their employees. In this case, how the organization (i.e. management) expects employees to act and behave when confronted with a phishing email or spoofed website. In this regard, Agency theory can be used with great effect and thus

defines the HO relationship. As employees (i.e. humans) will be confronted, directly and indirectly, with the technological controls introduced by the organization, it is important that they are made aware of their role towards ensuring that these controls are as effective as possible. They also need to be trained in how to use the technological controls to combat phishing. The TAM assists to ensure that the technological controls are accepted and used accordingly. This gives rise to the HT relationship.

In all three of the relationships discussed earlier, human involvement is apparent. Phishers most frequently exploit human behavior which is made easier by a lack of knowledge in the correct use of technology. Furthermore, humans' lack of compliance with organizational policies and procedures favors phishers. In order, therefore, to be adequately protected against phishing attacks, particularly in an organizational context, a framework is required whereby *all* the HOT relationships are working seamlessly with each other [8]. A security awareness programme aimed at addressing each of the relationships, can help achieve this. Security awareness, training and education can help change users' mind-sets and behavior towards information security thereby making them a more effective security defense in an organization [19]. In doing so, the number of security incidents can be reduced [20]. NIST 800-16 [21] describes the process of information security education as a continuum. This continuum is fairly widely accepted and consists of awareness, training and education [22]. This continuum is necessary for the successful implementation of any information security programme [21]. Learning in the continuum begins with awareness, develops into training, and finally evolves into education [21]. Furthermore, the role each individual plays in an organization determines and defines the IT security learning needed by that individual [21]. Components from ISO/IEC 27002 [23] were studied and taken into account in the context of phishing. The following subsections classify the educational components according to the three main sets of relationships under discussion, which aids to structure the educational components more logically. Aligning these three relationships will help reduce the gap that permits phishing threat agents to proliferate through the other relationships. Also, strengthening these three relationships can help create a holistic anti-phishing framework known as HOT.

A. Human-Technology Relationship

Technological controls play an essential role in the protecting of organizational information assets. Organizations and end-users apply a great deal of attention to the implementation and use of technological controls to combat general information security threats. Predictably, this approach has been expanded to combat phishing attacks. However, the success of technological controls depend on, to a certain extent, how humans interact with it. Technological controls are managed and used by humans, who if not trained may leave their system open to a phishing attack. Furthermore, technological controls themselves can also possess software vulnerabilities that phishers may exploit. To further add to this complexity, technology is constantly changing and, as such, users need to be frequently educated on these changes. It may be argued that users' lack of understanding in the use of such technologies is what exposes them to phishing attacks the most. Therefore, to address this, it must be considered that education should aim to enhance users' understanding of what the threat of phishing entails and also the most efficient ways in which technology can be used to combat this threat. To accomplish this, organizations would require an information security training programme.

1) Information security training

If organisations have the opportunity and resources, they can use a phased approach for training. For example, they could classify their training programme into two phases. Table 1 gives an example of this approach.

TABLE I. USING A PHASED APPROACH FOR INFORMATION SECURITY TRAINING IN PHISHING

PHASES	OBJECTIVES
Phase 1: Introduction to information security and modern security threat agents	To give users knowledge of the dangers security threat agents present for organisational assets. To distinguish between different types of security threat agents. To identify phishing emails and spoofed websites.
Phase 2: Technological controls used to combat phishing attacks	To give users the skills required to use technological tools correctly to combat phishing attacks

Phase 2 is of key importance, as it specifically addresses phishing. In this phase, users will require technical training in the various file types, web browser and system warning alerts, email client, logging off/locking workstations, anti-malware software and so on. The training must ensure that users check the URL in the address bar before logging into their account and to avoid unwittingly clicking on hyperlinks contained within emails. They must also ensure that the website is encrypted with a SSL certificate by considering the icon of a padlock or the 'https' protocol before the URL in the address bar when entering personal or financial information. Users should not provide any personal credentials or information as a reply to an email or on a pop-up page, as established institutions do not request such information in this manner. Besides gaining knowledge in the use of these technologies, the overall objective of this training is to influence attitudes towards technology by ensuring that technology and its security controls are experienced by all users as being useful and as easy to use as far as possible. This supports the TAM objectives and as a result can help strengthen the HT relationship.

B. Human-Organisation Relationship

This subsection focuses on educational aspects of the organization and how they govern information security in particular and its employees in general. This may appear to be irrelevant to phishing; however, it does have influence on the prevention of phishing incidents. Payne [24] states that statistics have proven that the most prevalent security gap affecting organizations are caused by insiders (i.e. employees), as opposed to external threat agents, such as hackers. Payne [24] points out that security gaps are mainly caused by the following reasons; (1) users are not aware of security threats,

(2) users incorrectly rely on someone else to treat security threats, for example IT personnel, (3) users are not adequately skilled in addressing threats and finally, (4) users feel that they have more important activities to be concerned about, for example their direct work tasks. Point (1) and (3) has been addressed in Section A. User education emerges as the solution to address these concerns. However, as pointed out by Payne [24], this is complicated when; (1) users do not acknowledge that it is their personal responsibility to ensure security, (2) users consider security too technically complex for them to understand, (3) top-level and middle-level management fail to comprehend the importance of information security and the threat that related risks poses to the organization and finally, (4) security budgets and staff are not utilized appropriately. From the factors described above, a number of concerns emerge. Humans have a negative attitude towards accepting personal responsibility for ensuring information security and furthermore, they are not adequately educated to deal with security threats under all circumstances. More concerning is that top management is not necessarily setting an example in taking security risks more seriously. Consequently, users in an organization develop attitudes from the preconceived ideas that security issues should be treated more as a technical concern and is thus the responsibility of technical staff. This in turn then influences their behavior and furthermore, the resultant organizational information security culture. The concept of agency theory posited that employees and the organization often have conflicting needs [25]. These conflicting needs may be a result of an employee's attitudes, behavior or personal needs. In this relationship, much attention is paid to the factors that affect user behavior, specifically the changing of attitudes and behavior towards the best interests of the organization. This is particularly important because phishers take advantage of ignorant or irresponsible human behavior. For example, while at the organization employees are supposed to be engaged in work-related activities, and not participating in social networking websites that may create opportunities for phishers to target them. If an employee's behavior is not managed at the correct level, the organization can be at risk of security threats, which most definitely include phishing.

ISO/IEC 27002 [23] classifies this HO relationship as human resources security. Similarly, COBIT 4.1 [26] describes it as IT human resources management. In comparing the principal and agent entities described in agency theory, the stakeholders affected in this relationship are the *organisation* and its *employees*. Top-level management and human resource management represent the organisational aspect and management is, typically, entrusted with formulating these policies. The 'employee' aspect consists of all other staff on whom organisational policies and procedures are imposed. The following subsection describes what needs to be done to ensure that organisational policies and procedures are drafted and complied with.

1) Organisational Policies and Procedures (including the Information Security Policy)

One method organisations use to enforce practice in information security, is through its policies and procedures. The drafting of policies and procedures is vital to such an extent that COBIT 4.1 [26] and ISO/IEC 27002 [23] regard this as core to the relationship between the organisation and its employees. Policies and procedures define the relationship between the organisation (i.e. management) and its employees. More importantly, these policies and procedures dictate employee behaviour in the organisation [27]. For a change in behaviour to take place, employees need to firstly be made distinctly aware of policies and procedures. Merely validating that policies have been read, does not change human behaviour. As such, it is important that all users in the organisation, including contractors and third-party users, should receive appropriate security awareness training as well as regular updates in organisational policies and procedures, as are relevant for their job function [23]. If this is achieved, there may be fewer opportunities for phishers to exploit human behaviour.

Herath and Rao [28] suggested that research and field surveys suggest that employees seldom conform to information security procedures. Unfortunately, information security policies are not taken seriously enough because they are seen as mere guidelines or general directions to follow rather than actual rules [28]. As a result, research in information security behavior has started focusing on employees' intentions to conform to security policies. It has been revealed that even in cases where users have knowledge of a specific security policy, they may still deliberately ignore it because they do not understand why it is needed [22]. Furthermore, organizations do not put more resources into educating their employees in policies and procedures. Instead, the traditional approach used by organizations is to merely inform their employees that they have policies and it should be obeyed or else they will consequently face disciplinary action. However, this approach is not likely to increase employee motivation or improve attitudes [29]. This will consequently put the organization at risk as users will not necessarily behave securely in the organization [18]. Seen in the context of agency theory, it may be more sustainable to help employees understand *how* their actions in protecting information assets will empower them, instead of just making them follow orders [30].

Awareness and training relating to the organisation's policies and procedures must be carried out before user access and services are granted [23]. This can be done on appointment of employees, and then be continued on an ongoing basis. Furthermore, it should inform employees of known security threats, who to contact for further security advice and the proper channels for reporting security incidents [23]. A security awareness programme must ensure that employees understand how their behaviour may endanger the information assets of the organisation and also how this can 'personally' affect them. This requires employees to be educated in activities that are regarded acceptable and unacceptable by the organisation, details which can be outlined in organisations' security policy documents. Employees require training in the security threats and protection methods that were addressed in the information security training that addressed the HT relationship. Once employees have been educated in this regard, they will understand the importance of policies and procedures and will therefore be positively influenced to abide by them.

To further enhance awareness of security policies and security threat agents, the organisation can place security

posters conspicuously in offices and corridors. These posters will make employees aware of crucial points in policies, as well as modern security threats. Thus, the opportunity is created for employees waiting for a meeting or having a tea break to read these posters. In this regard, awareness is used to continually remind people to comply with organisational policies. Employees should understand that it is their responsibility to acquire knowledge of the organisation's policies and procedures and they should not plead ignorance when accused of misconduct in this regard. Hence, employees should understand that the organisation can institute disciplinary proceedings if policies are not followed, regardless whether the misconduct was unintentional. This could be addressed by a general misconduct policy which further describes the procedures for the disciplinary process.

This subsection suggested that, by educating employees on the purpose of security policies, employee attitudes, work ethic, knowledge and behaviour can be positively influenced. Motivation will play a vital role in ensuring that employees perform their tasks at an acceptable level. This statement is supported by ISO/IEC 27002 [23], which states that motivated personnel are likely to be more reliable and as a result will be less inclined to cause security incidents. However, there are other factors worth mentioning that also have an influence in strengthening the relationship between the organisation and its employees. ISO/IEC 27002 [23] expresses these factors as human resources security. These factors are generally targeted at recruiting trustworthy staff and influencing their behaviour towards the needs of the organisation. If these factors are also not managed correctly, they can also pose security risks to the organisation. These factors include the following:

- *Recruitment process for new staff members* – interviews, background security checks/screening, employing suitable candidates that are qualified and/or experienced.
- *Job description* – integrating information security into job descriptions. Employees will then recognise that it is their responsibility to ensure information security. Clearly defined roles can have a significant impact on people attitudes [14].
- *Skilled staff* – it is important for staff to possess the skills needed for their job responsibilities. If staff members are not adequately skilled for their tasks, they may pose security risks to the organisation. The Deloitte cyber security study revealed that a lack of skilled staff remains one of the top concerns for organizations [1].
- *Employment contract* – employees understand and agree to binding organisational policies
- *Induction/orientation programmes* – extensive security briefings in policies, security procedures and access levels, training in the use of information systems
- *Fair compensation* – employees will feel that they are treated fairly if they receive adequate monetary compensation for their work [14]. Incentives can also be used to reward employees for their work performance, as well as to motivate employees.
- *Monitoring and evaluation* – incorporating information security evaluation as part of job performance evaluation. Furthermore, monitoring Internet usage in order to protect the organisation's internal systems from threats.
- *Termination or change of employment* – often referred to as an exit strategy, is the removal of employee access rights, including physical and logical access, keys, identification cards and information processing facilities. This includes the returning of assets supplied by the organisation. A formal disciplinary process for misconduct must be undertaken.

The method in which these factors are implemented and managed can be described in organisational policies and procedures. Poor management may result in employees feeling undervalued, thus having a negative impact on the organisation in terms of security [23]. For example, poor management may lead to security being neglected or the potential abuse of the organisation's assets. Ideally, if employees are motivated they will treat information security programmes differently, as they understand that the objective of having such programmes is to protect both them and the organisation. The survival of the organisation is dependent on its employees support and vigilance toward organization policies and procedures. If this does not happen, it can potentially put the organization at risk to phishing attacks. Employees should be mindful of the disciplinary action the organization can take against them, should they fail to comply with policies. Accordingly, employees should also be educated in this regard.

C. Organisation-Technology Relationship

COBIT defines requirements for the control and security of sensitive data and therefore provides a suitable guideline to addressing the OT relationship. It is the organisation's responsibility; in particular management, to ensure that technology is introduced, utilized correctly, maintained, and secured from internal and external threat agents. In this respect, COBIT is a best practice that can ensure that phishing is suitably addressed by the organization. The following subsections discuss components taken from COBIT which can help combat the phishing threat in the context of the OT relationship.

1) Communicate Management's Aims and Direction

Firstly, the organisation (i.e. management) should develop an organisational IT control framework and communicate policies. To accomplish this, management must approve and support an awareness programme to express its mission, service objectives and policies and procedures. Achieving this will ensure accurate and timely information on current and future IT services, the associated risks and the responsibilities of staff.

2) Ensuring Systems Security

The organisation's security should be managed at the highest appropriate organisational level. This is to ensure that security actions are aligned with business requirements [26].

The IT security plan must be implemented in organizations' security policies and procedures, together with suitable investments in services, personnel, software and hardware. The CEO should be informed of this process and the security policies and procedures should be communicated to all stakeholders. A management process is required to establish and maintain IT security roles and responsibilities, standards, policies and procedures. Therefore, management should ensure that technical staff is trained to implement up-to-date security patches and anti-virus solutions to protect the organization's information systems and technology from malware (viruses, worms, spyware, spam, etc.) and phishing. The organization should ensure that its security-related technology is protected from tampering and damage. Network security should be in place (e.g. firewalls, and intrusion detection systems) as this may be an entry point for phishing attacks. Security controls must be used to authorize access and control information that flows in and out of the organizational network. Furthermore, it should be assured that the organization's data transactions are exchanged over trusted paths or media. Controls should be in place to provide authenticity of content, which is particularly important for customers who engage in online banking, which is a concern for phishing victims. The organization should also ensure that it's critical information is withheld from unauthorized users (i.e. social engineers and phishers) and that measures are in place to protect and recover information in the case of system failures, human error, disasters or deliberate attacks. For the organization to ensure that the requisite activities are carried out, the organization should

- understand security requirements, vulnerabilities and phishing threat agents
- manage user identities and authorizations in a consistent manner
- assess its security levels frequently.

3) Monitor and Evaluate Internal Controls

Phishing has damaged the reputation of many reputable organisations. To prevent this, the organisation can measure its security levels by the number of security incidents affecting the public and themselves. This will include the monitoring and evaluation of internal controls. The organisation should ensure that the security controls it has in place to combat phishing attacks are monitored regularly by the appropriate staff to ensure their effectiveness. The cyber security study by Deloitte [1] revealed that only 8% of organisations (i.e. CISO) actually measure the value and effectiveness of their respective organisation's security activities. Any security concerns should be reported to management for any further intervention.

4) Establish Regulatory Compliance

Compliance also plays a role in IT governance. This is supported by [31], who state that "[r]egulatory compliance is one of the core governance disciplines". To ensure positive compliance and to reduce the risk of non-compliance with IT laws and regulations, an independent review process is necessary. Such as a process includes defining an audit charter, auditor independence, professional ethics and standards, planning, performance of audit work, and reporting of and following up on audit activities. To ensure compliance, the organisation should firstly identify IT-related legal and regulatory requirements, then assess the impact of regulatory requirements and, finally, monitor and report on its compliance with regulatory requirements. In this regard, COBIT can be used as a starting point to meet this objective.

By taking into account all of the components discussed above in each of the relationships, Fig. 1 below, illustrates the HOT framework with its associated theories and best practices.

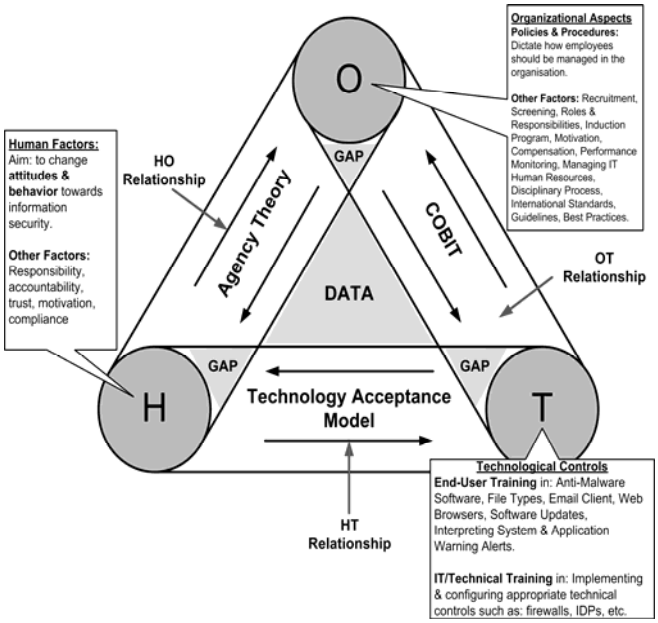

Figure 1. HOT Framework and its components

The relationships between the HOT elements need to be tightly bounded. Failure to achieve this creates security "gaps" which will consequently allow phishers to target these vulnerabilities. Strengthening the HO relationship can be addressed by educating employees on the organisation's policies and procedures. The HT relationship can be strengthened by means of an information security training focusing on the use of technological tools used to combat phishing. This type of training will affect all employees at different levels of the organisation. Finally, the OT relationships can be strengthened by ensuring that top level management supports an organization-wide security awareness programme, it has the appropriate technological tools to combat phishing and that it is continually monitored and evaluated for its effectiveness. Finally, the organisation must comply with IT laws and regulations. The following section discusses the research process followed and the results from evaluating the HOT framework for its usefulness and completeness.

IV. Evaluation of Anti-Phishing Framework and Results

In this study Hevner et al.'s [32] design science guidelines were used to assist in the design of the HOT (Anti-Phishing) framework. Research in the field of information systems can

typically be divided into two paradigms, namely, design science and behavioral science [32]. The design science paradigm aims to extend the boundaries of human and organizational capabilities by creating new and innovative artefacts to solve an identified organizational problem [32]. This requires knowledge and understanding of a problem domain and the solution to the problem is achieved through the construction and application of the designed artefact. The artefacts are then evaluated in terms of the utility they provide in solving those problems [32]. In this study, the problem domain encompasses the fact that phishing threat agents penetrate organizational security controls by exploiting human behavior. To address this problem, a behavioral science paradigm would seek to develop and verify theories that explain or predict human or organizational behavior. In this study, the behavioral paradigm focused on identifying suitable theories and best practices, such as the TAM, Agency Theory and COBIT, to help understand human behavior in each of the HT, HO and OT relationships. Hence, the aim was to help strengthen the organization's security defenses by focusing on educating humans in each of these areas. This study has made use of both paradigms. This is supported by [32], who believe that both paradigms are fundamentally necessary for understanding people, organizations and technology. Indeed, the elements cited by [32] coincidentally relate to the same foundations used in this study, namely, the human factors, organizational aspects and technological controls.

Evaluation is a vital component of the research process [32]. The business environment establishes the requirements upon which the evaluation of the artefact is based. Hence, the HOT framework was evaluated by personnel responsible for security in their respective organizations. This satisfies Hevner's [32] third guideline for 'design evaluation'. In this respect, IT artefacts can be evaluated in terms of their functionality, completeness, consistency, accuracy, performance, reliability and usability in the organization environment. In this study, the aim is to establish the perceived usefulness (usability) and completeness of the IT artefact (i.e. HOT framework) in the business environment. Accordingly, a design artefact is complete and effective when it satisfies the requirements and constraints of the problem it was meant to solve. In this study, the problem is to effectively educate humans to prevent them from falling victim to phishing attacks.

Hevner et al. [32] categorize the evaluation methods that should be aligned appropriately to the designed artefact and the selected evaluation metrics. For this purpose a 'descriptive' evaluation method is used that includes 'informed argument' and 'scenarios' and both of these were applied to this study. Using the informed argument principle, information from relevant research was used to build a convincing argument for the need for an anti-phishing framework. Scenarios, discussed by [8] were taken into account to demonstrate the gaps in each of the relationships caused by human involvement. This contributed towards the development and utility of the HOT framework (artefact).

A purposive sample of three well established organizations in East London, which offer IT/security related services to their clients, were chosen. The services these organizations provide include: risk assessments, IT auditing, information management, network security, outsourcing, financial services, cloud services and so on. Senior staff members responsible for information security in these three organizations were selected to evaluate the components of the anti-phishing framework during semi-structured interviews. All participants have sufficient experience in the information security field and also have management experience. These three organizations were classified as Company A, B and C respectively. The objective of the interviews was to verify if the components discussed in the framework, would serve as an improved defense model against phishing threat agents. The interviews were arranged beforehand with the participants who scheduled a time that was suitable for them at their respective organization. A semi-structured interview was chosen as the appropriate research method, as it is flexible and allows new questions to be asked during the interview process in response to what the interviewee says [33]. An interview guide, containing prearranged questions, was used in the interviews. Participants gave permission for the conversations in the interview to be recorded. Note-taking was also used to record relevant key points during the interview [33]. Diagrams were provided in the interview which helped respondents in terms of giving them a graphical representation of the HOT framework. The diagrams illustrate the framework's beginnings as a single-layer defense model and its ultimate development into a multi-layer defense model. Their responses were grouped according to the interview questions as per organization. From this, main themes were established that further synthesized the findings.

After explaining in detail human factors, organizational aspects and technological controls in the context of phishing, all interview respondents agreed that all three relationships should be considered in forming a suitable defense (i.e. a HOT framework) against phishing. All interview respondents agreed that each of the three HOT relationships is operating in isolation from one another, thus forming only a single-layer defense against phishing. However, Company C felt that the relationships are not 'completely' isolated from each other, but certainly they need to be improved in terms of cooperation. As such, all participants stated that a holistic model is needed to address phishing instead of one comprising a single-layer defense. All respondents, without hesitation, felt that some form of security awareness, training and education programmes is necessary to strengthening each of these linkages in order to reduce this gap between each of the relationships. Company A pointed out that even if technology fails and users ignore policies, the human element is still the point of entry where most security weaknesses occur. As such, Company A felt that the human element requires awareness raising and training to address these concerns. Company A maintained that the best way for an organization to educate users on phishing is to carry out mock tests without the knowledge of its employees. The respondent added that induction programmes, brochures, flyers, emails, intranet, and posters on walls are all methods that make employees aware of pertinent security issues. However, Company A stated that, although people may read the information, they will only internalize it once they have suffered the consequences of a policy breach. Therefore, Company A's approach is to conduct external threat assessments of their employees by sending them phishing emails. Company A also believed that the organization can

implement firewalls and block certain websites to a certain extent; nevertheless, users will try to circumvent these controls. Company A felt that informing employees that the organization has technological controls in place is even more risky. Instead, the respondent maintained that users should rather be informed about the technological controls the organization has in place and the extent of the protection they offer and where the risks lie thereafter. The respondent further added that, today, phishing emails and spoofed websites are so sophisticated that even employees of Company A were unable to distinguish such emails as phishing attacks.

All respondents were not familiar with the TAM and agency theory. However, after having explained the theories, they accepted that they all fit the context of each of the relationships appropriately. All respondents agreed that information security training is necessary to address the HT relationship and should be classified into different user levels. Additionally, Company C stated that, should there be an instance where a new technology or feature is introduced, then employees would be trained accordingly. Moreover, members of top management who do not necessarily have the required security knowledge should be given basic information security training. One of the reasons for this is to lend management support for such programmes.

In addressing the HO relationship with policies and procedures, Company A specifically felt that human behavior is so complex that for awareness of policies to be effective, they should be made more personal for employees; in other words, how the consequences of disobeying policies can affect them personally, for example, in terms of loss of income. Company C believes that policies and procedures must exist as they set the boundary or scope of what employees are expected to do and how they do it. However, Company C felt that this is still uncontrollable. Company C elaborated more on this with by mentioning the following example: A working hour's policy requires that an employee must work from 8:00 to 17:00 every day. However, employees can choose to work slowly during this period. Accordingly, employees' ethics and behavior become an issue. Thus, even though there may be boundaries created by the policies, people are still able to make decisions within those boundaries which consequently indirectly violate what the organization expects from their employees. Company C felt that employees are not likely to respond to policies unless there is a major consequence or reward. As such, Company C believes an awareness programme can inform users on these two aspects so that they can influence their behavior. Company C felt that if employees behave in the best interests of the organization, then they should be rewarded. Consequently, they can be used as an example to other users and therefore help to grow the security culture. Company C stated that comprehensive policy documents will not be read and, furthermore, that too much information given too quickly is not desirable. The respondent further stated that the amount of information people can internalize is limited. Therefore, they felt that it is beneficial to give less information to users but more often. They also felt that raising awareness in terms of policies should not happen once, but should take place on a constant basis. They felt that actual training on policies will not be effective because the very nature of a training workshop may imply that training will take a few days and, as a result, will demotivate employees. As a result, Company C supports short work sessions during which employees are made aware of certain security aspects. This would indicate that training takes less time and users understand what to expect. In terms of policies, users should be made aware why they are in place and management should be able to justify the policies instead of taking an approach of "this is what you can or cannot do".

All respondents have experience in the use of COBIT and as such, supported that COBIT is the appropriate relationship between O and T. All respondents were inclined to select many of the guidelines offered by COBIT to address phishing. Companies A and B selected monitoring and evaluation guidelines ME2. Company C felt that merely ensuring systems security is an operational item and can lose its importance over time if it is not regularly maintained. Company C therefore felt very strongly that monitoring and evaluation guidelines (ME2 and ME3) should be favored above all other COBIT guidelines. They felt that putting in place (i.e. delivering) technological controls is relatively simple, but if these controls are not monitored their effectiveness will decrease, especially since such technological controls are constantly evolving. Company C mentioned that there needs to be some level of feedback on the control levels and that if monitoring is performed, then the outcomes from monitoring will determine what areas need to be addressed through security awareness, training and education programmes.

Respondents could not further contribute any other components that could be considered in the HOT framework. When asked, if ISO27002 could serve as an additional component in the HOT framework, all respondents felt that it should not be a separate component of the relationships. Company C stated that such best practices "live" in each of the relationships.

On the question of whether the HOT framework will help to protect an organization against phishing attacks, Company A and B supported the notion that strengthening the three main relationships can certainly help towards addressing the phishing problem. Company C felt that integrating the HOT aspects would certainly be effective in improving the organization's current risk level. However, Company C felt that there would a need for an implementation strategy for the security awareness and training components to be put in place. Table 2 below summarizes the key findings of these interviews.

TABLE II. SUMMARY OF KEY FINDINGS

SUMMARY OF KEY FINDINGS
All three HOT relationships in an anti-phishing framework are required to combat phishing.
Security awareness, training and education are necessary to strengthen each of the relationships.
Ongoing awareness, using the requisite methods, of organisational policies and procedures must be made personal to employees.
All users should receive security training related to their roles and responsibilities.
Monitoring and evaluation of the organisation's technological controls should be performed regularly.
Management should openly demonstrate their support for information security.
An implementation strategy for each of the three relationships is necessary.

V. CONCLUSION

This paper described an approach to combatting phishing by classifying phishing controls into relationships. These relationships needed to be improved upon through educational strategies. The HT relationship defined an information security training programme aimed at training end-user staff in the use of technological controls to combat phishing threats and the identification of phishing threat agents. Technical staff training is necessary to ensure that the organization applies the appropriate tools to combat phishing threats. Moreover, top management requires training to understand their responsibility in the protection of the organization's information. The aim of such training is to convince management that their responsibility towards security is not limited to technical staff or the IT department. The HO relationship is concerned with the organization's management of employee behavior. The introduction of policies and procedures is one method used by organizations to ensure that their employees demonstrate the correct behavior. However, employees are often unfamiliar with such policies, and therefore do not understand why it is needed. As such, policies and procedures should be communicated to employees through an awareness campaign. Such a campaign will ensure that employees understand the policies and procedures in place, know where to locate them and understand their importance in terms of their safety and of the organization. Whitman and Mattord [34] recommend that a set of tests or quizzes can be developed to determine if employees understand key points covered in the information security policy. In the OT relationship, management has to ensure that it has the requisite staff and technological tools to support the organization and protect it from phishing attacks. Technical staff will require training in this regard but raising ongoing awareness will also ensure that all staff is aware of their roles and responsibilities. Ensuring enterprise security is even more important for organizations providing a service to their customers. In such cases if customers' information is compromised in any way, it would consequently affect the organization's reputation. Financial institutions, affected by phishing, know too well how the latter has affected their revenue.

REFERENCES

[1] Deloitte, *Deloitte-NASCIO Cybersecurity Study: State governments at risk: a call for collaboration and compliance*, 2012, Available: http://www.nascio.org/events/2012Annual/documents/State-Governments-at-Risk.pdf [Accessed 20 November 2012].

[2] E. Harper, "Watch out for Warlords of Draenor phishing scams," 16 April 2014, [Online] Available: http://wow.joystiq.com/tag/scams/ [Accessed 17 April 2014].

[3] Business Standard, "Phishers create fake FB ID of Kejriwal," 16 April 2014 [Online], Available: http://www.business-standard.com/article/current-affairs/phishers-create-fake-fb-id-of-kejriwal-114041500814_1.html. [Accessed 17 April 2014].

[4] ITWeb, "SA - hotspot for phishing attacks," 29 April 2014 [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=134134:SA-hotspot-for-phishing-attacks&catid=265 [Accessed 30 April 2014].

[5] APWG, "Global Phishing Survey:Trends and Domain Name Use in 2H2013," 10 April 2014 [Online], Available: http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf [Accessed 16 April 2014].

[6] C. Pash, "You're Most Likely To Be Targeted By A Phishing Scam On A Wednesday," 14 April 2014, Available: http://www.businessinsider.com.au/youre-most-likely-to-be-targeted-by-a-phishing-scam-on-a-wednesday-2014-4#ixzz2z2EPSii8 [Accessed 16 April 2014].

[7] E.D. Frauenstein and R. Von Solms, "Phishing: How an organisation can protect itself," in *Proceedings of Information Security South Africa (ISSA) 2009*. Johannesburg, South Africa, 2009, pp. 253–268.

[8] E.D. Frauenstein and R. Von Solms, "Using theories and best practices to reduce the phishing gap," European Information Security Multi-Conference (EISMC*)*, in *Proceedings of Human Aspects of Information Security & Assurance (HAISA) 2013 conference*. Lisbon, Portugal, 08-10 May 2013, 2013, pp. 69-78.

[9] F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, 13, 1989, pp. 319–340.

[10] K.M. Eisenhardt, "Agency theory: An assessment and review," *Academy of Management Review*, 14, 1989, pp. 57–74.

[11] J. Luftman, *Strategies for information technology governance*, Pennsylvania, USA: Idea Group, (IGI Global), 2004.

[12] M. E. Thomson and R. Von Solms, "Information security awareness: Educating your users effectively," *Information Management & Computer Security*, 6, 1998, pp. 167–173.

[13] K. Aytes and T. Connolly, "Computer security and risky computing practices: A rational choice perspective," *Journal of Organizational and End User Computing*, 16(3), 2004, pp. 22–40.

[14] D. Lacey, *Managing the human factor in information security: - How to win over staff and influence business managers*, West Sussex, England: Wiley, 2009.

[15] J.S. Downs, M.B. Holbrook and L.F. Cranor, "Behavioral response to phishing risk," in *Proceedings of the Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit*, Pittsburgh, Pennsylvania. 1299019: ACM, 2007, pp. 37-44.

[16] J. Leach, "Improving user security behaviour," *Computers & Security*, 22, 2003, pp. 685–692.

[17] M.A. Sasse, D. Lawrence, L. Coles-Kemp, I. Flechais and P. Kearney, "Human Vulnerabilities in Security Systems," *Cyber Security KTN Human Factors* (White Paper), 2007, Available: http://hornbeam.cs.ucl.ac.uk/hcs/publications/HFWG%20White%20Paper%20final.pdf [Accessed 12 March 2010].

[18] J.F. Van Niekerk, "Establishing an information security culture in organizations: An outcomes based approach," Magister Technologiae: Information Technology, Nelson Mandela Metropolitan University, 2005.

[19] E.C. Johnson, "Security awareness: Switch to a better programme," *Network Security*, 2006, pp. 15–18.

[20] S.D. Hight, "The importance of a security, education, training and awareness program," 2005 Available: http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf. [Accessed 02 September 2012].

[21] NIST 800-16, *Information technology security training requirements: A role-and performance-based model*, Gaithersburg, MD: National Institute of Standards and Technology.1998.

[22] T. Schlienger and S. Teufel, "Information security culture: From analysis to change," in *Proceedings of the 3rd Annual Information Security South Africa Conference (ISSA).* Johannesburg, South Africa, 2003, pp. 183–196.

[23] ISO/IEC 27002, *Information Technology: Security techniques – Code of practice for information security management.* ISO/IEC 27002:2005. Standards South Africa. 2005.

[24] S. Payne, "Developing security education and awareness programs," *Educause Quarterly*, 4, 2003, pp. 49–53.

[25] M. Jensen and W. Meckling, “Theory of the firm: Managerial behavior, agency costs, and ownership structure,” *Journal of Financial Economics*, 3, 1976, pp. 305–360.

[26] COBIT 4.1, *COBIT 4.1 Executive Summary*, Illinois, USA: IT Governance Institute. 2007.

[27] K.D. Mitnick and W.L. Simon, *The art of deception: Controlling the human element of security*, New York, NY: Wiley. 2002.

[28] T. Herath and H. R. Rao, “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decision Support Systems*, 47, 2009, pp. 154–165.

[29] M. Siponen, “A conceptual foundation for organizational information security awareness,” *Information Management & Computer Security*, 8(1), 2000, pp. 31–41.

[30] L. Du Plessis and R. Von Solms, “Information security awareness: Baseline education and certification,” in *Proceedings of Information Security South Africa (ISSA) 2002*, Muldersdrift, South Africa, 10-12 July 2002.

[31] E.J. Brown and W.A. Yarberry Jnr, *The effective CIO: How to achieve outstanding success through strategic alignment financial management & IT governance*, New York: Auerbach. 2009.

[32] A. Hevner, S.T. March, J. Park and S. Ram, “Design science in information systems research,” *MIS Quarterly*, 28, 2004, pp.75–105.

[33] C. Dawson, *Practical research methods: A user-friendly guide to mastering research*, United Kingdom: HowtoBooks. 2002.

[34] M.E. Whitman and H.J. Mattord, *Management of information security* Canada: Course Technology/Cengage Learning. 2010.