# The Three Dimensions of Security

**Malik F. Saleh**
msaleh@pmu.edu.sa
*Management Information Systems, Chair*
*Prince Mohammad Bin Fahd University*
*Al Khobar, 31952, Saudi Arabia*

**Abstract**

Security is an issue of generally recognized importance. Security starts with you, the user. It is well known that a formal security policy is a prerequisite of security. Having a policy and being able to enforce it is a totally different thing. This paper explains the three aspects of security that should be combined to create a well-rounded solution for securing organizations. This solution examines people, policy and enforcement as three dimensions in the world of security. This paper serves as 1) a conceptual framework for securing organization 2) the basis for formal policy-to-enforcement; 3) It raises awareness that the users should be informed of their roles and responsibilities in protecting the organization; and 4) evidence for writing policies that can be implemented and enforcement involves understanding the policies by the users.

**Keywords:** dimensions of security, Security, Policy, People, enforcement of security.

## 1. INTRODUCTION

Security is an issue of generally recognized importance. Protecting an organization means securing the organization. Security is achieved from the prevention of attacks and from achieving the organization's mission despite attacks and accidents. The traditional information security objectives are confidentiality, integrity, and availability. Achieving these three objectives does not mean achieving security [1].

It is well known that a formal security policy is a prerequisite of security. Having a policy and being able to enforce it is a totally different thing. The security policy is the first line of defense. Without a well-designed policy, the security of the system becomes unpredictable and governed by the system administrator [2]. Employees are the greatest threat to an organization's security. Their non-compliance with security policies not only threatens the integrity of the system, but also costs the organization a significant amount of money due to the loss of information or due to fixing problems that the user causes [3]. Therefore, Security starts with you, the user.

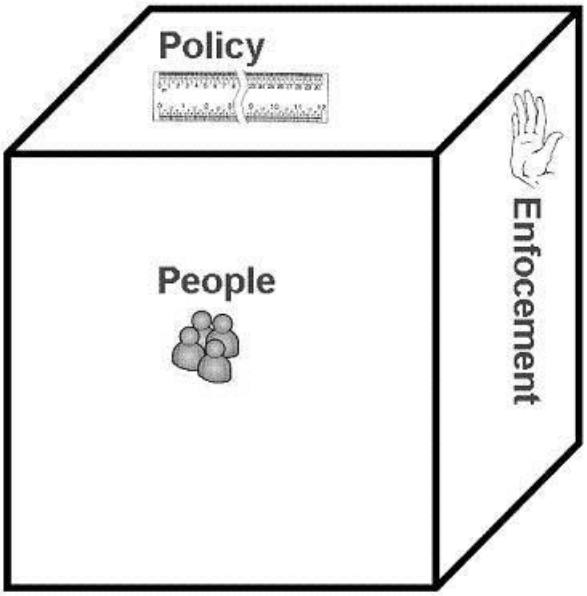
Does added security make things more difficult to use? Will people always resent the extra steps? Norman [4] argues that the answer to both questions is the same: not necessarily. Both are design issues that require understanding of the need for security and the workings of the mechanisms that enforce them. We tolerate the added security because it seems necessary and the amount of effort it demands usually seems reasonable.

Effective policy enforcement involves many steps such as ensuring that the policies are understood by all the users, regularly checking to see if the polices are being violated, and having well-defined procedures and guidelines to deal with incidents of policy violation [3] . Looking at protecting the information at an organization we found that all organizations share a common risk, the users. To achieve security, different elements in this risk should be dealt with individually as well as in unity.

This paper explains the three aspects of security (see Fig.1) that should be combined to create a well-rounded solution for securing organizations. This solution examines people, policy and enforcement as three dimensions in the world of security. It serves as 1) a conceptual framework for securing organization 2) the basis for formal policy-to-enforcement; 3) It raises awareness that the users should be informed of their roles and responsibilities in protecting the organization; and 4) evidence for writing policies that can be implemented; and enforcement

involves understanding the policies by the users. In order to make effective protection, organizations need to have an overall policy. That policy needs to be implemented in multiple ways and it should be a simple policy.

Figure 1: The Three Dimensions of Security




## 1. BACKGROUND AND RELATED WORK

Users, policies, and enforcement are important topics for the security and audit community and each part has received a fair amount of research attention. To frame the discussion on the combination of the three parts, we categorize the prior research into work that addresses each part individually but in relation to the other parts. We also discuss research from the computer policy community and the availability of enforcement products from different vendors.

The motivation for this paper was due to the challenges of enforcing policies on the users that the users don't understand. We acknowledge that security is still heavily reliant on technological solutions, but the vulnerability and the risk is attributed to the users. We argue that these challenges are due to writing policies without getting users involved in policy writing and due to lack of training to the users. Further, policies should inform the users of their roles and responsibilities in protecting the organizational assets.

This paper is organized in different sections. Section 2 discusses briefly the related work and the fact that each of the users, the policy and enforcement are covered in detail in the literature. Section 3 examines the users; section 4 examines the policies in relation to the users. Section 5 examines enforcing policies on the users. We conclude that the three dimensions of security are of a non-technical nature. All these dimensions must be taken into account in designing and creating a comprehensive information security plan for organizations.

## 1. THE PEOPLE DIMENSION

Who are the users? According to [5], the users are the enemy. The interaction between the users and the system is responsible for the functioning of the system and in most cases, this very interaction, according to [6], is the greatest risk. The threat posed by legitimate users in an organization has been labeled as "The Enemy Within" [7]. Most users put their firms at risk through either their sense of security or their ignorance. A small minority of users are believed to be actively seeking to damage the company from within [7]. Figure 2 explains this risk.

**Figure 2: Issues affecting security**


According to [8] the users are not the enemy. Users are often told as little as possible because they are seen as "inherently insecure." The inadequate knowledge lies at the root of users' "insecure" behaviors. Users perceived threats to the organization to be low because of their own judgments and because their roles in the system was not important

Many users do not understand the technical issues associated with privacy and security management [6, 9]. User behavior plays a part in many security failures, and it has become common to refer to users as the "weakest link" in the security chain [10]. Blaming the users will not lead to effective security systems. To address the weakest link in the security chain, organizations have to address this issue by transforming the end-users from users of the system to the enforcers of security by training end-users on security related issues. In general, users tolerate the added security because it seems necessary and the amount of effort it demands usually seems reasonable.

Phishing attacks that exploits user vulnerabilities rather than taking advantage of system vulnerabilities, take advantage of users' inability to distinguish legitimate company websites from fake ones. A great deal of effort has been devoted to solving the phishing problem by prevention and detection of phishing emails and phishing Web sites [11]. With all these efforts, phishing is still an issue for users and organizations. Automated detection systems should be used as the first line of defense against phishing attacks, but since these systems are unlikely to perform flawlessly, they should be complemented by warning users about the threat, through toolbars and browser extensions, and training users not to fall for attacks.

Research shows that training continues to have a significant organizational impact. Surveys have also found that the computer literacy requirements have skyrocketed in almost every end-user category. End-user training has three phases: initiation, formal training and learning, and post-training [12,13]. For security related issues, a discovery and disclosure approach should be followed. The disclosure should provide users with a sense of security that raises their awareness of the threats that their information systems face. While the discoverer may never disclose the finding, it educates the users. According to [13], the post-training phase has focused on the evaluation of training and learning immediately after training. However, organizations are more interested in long-term effects of training and the areas of end-user learning, rather than training. Organizations want to know if the training has been transferred to the workplace, and whether learning continues after formal training has ended.

Training according to [14] should:

1. Change the way the users think and act when it comes to security
2. Measure the success of the training program and
3. Continually address the importance of security.

The training program should consist of static topics that will be evaluated on a yearly basis, while a dynamic monthly component would consist of topics that were relevant at the time. Both components of the training are solicited opinions from different stakeholders. The idea of getting users involved in security related issue has a long-term impact on the culture of the organization and it will enforce all security policies of the organization.

## 1. THE POLICY DIMENSION

It is well known that formal security policy is a prerequisite of security. According to [15] the security policy is a direction-giving document for security within an organization. The policy defines the role information security has to play in reaching and supporting the organization's vision and mission. It should complement the organization's business objectives and reflect management's willingness to operate the organization in a controlled and secure manner. If a special-purpose security policies is defined, it is according to [16], perhaps best explained in terms of the principle of least privilege which holds that each user be granted the minimum access needed to accomplish their task. End-users therefore, will have the least privileges in the organization, but does a one size hits all work for all end-users!

It is argued [3] that policies should be written so that they are clear, concise and easy to understand. A security policy should be measurable, achievable, realistic, traceable and enforceable. Vague policies will increase the occurrence of non-compliance. Therefore, the security policy should inform the end-users of their roles and responsibilities in protecting the organizational assets. It is also argued by [15] that the roles and responsibilities in the security policy is one of the most important components of the policy, as this part tells exactly what is expected of users in terms of information security in the organization. The roles and responsibilities should cover all aspects of information security, as well as the individual responsibilities of all parties using the organization's information resources.

For example, the Security rule codified in the Code of Federal Regulations (CFR) has special information security implications that cannot be ignored. A comprehensive security awareness and training program is delineated as a standard to meet, with periodic updates as part of the program. Further, the CFR addresses controls that involve personnel, including clearance procedures for hiring and termination, and other human resources related matters [17].

Two challenges are faced when writing policies in natural language and implementing the technical details. First, the design of policy languages that allow flexibility and maximum expressivity is a popular research direction. In order to have all representation from different stakeholders when writing security policies, it is important to use flexible policy languages to demonstrate that a wide range of enforceable policies that can be specified [18]. Second, end-users are not technical to know the details of the policy therefore users have to approve the implemented policy by testing the implementation and experiencing the impact on their work.

There are a growing number of strict security and privacy audit and compliance requirements. This creates a need for policy-based systems [18]. Although an information security policy is a vital part of an organization's strategy for achieving information security, it is not always easy to put this document together. There are often differing opinions within the organization as to what constitutes a policy [15]. Organizations create policies to eliminate risk. Assessing risk can be seen as a three-phase process: identification, estimation, and evaluation. In the security world, the entire risk assessment process is called certification. Certification includes identification of risks, estimation of the consequences of accepting the identified risks, and evaluation of proposals for mitigating those identified risks [19]. Therefore the more strict the policy, the less risk organizations are willing to take for their

resources.

## 1. THE ENFORCEMENT DIMENSION

One of the deadly sins of information security according to [20] is not realizing that the protection of information is a business issue and not a technical issue. Information security enforcement is an essential and integral part of corporate governance. The driving force for making security part of corporate governance has seen several documents on corporate governance such as the ISACA's Control Objectives for Information and Related Technologies (COBIT). These documents have been supported by a growing set of laws and legal requirements. Organizations implementing COBIT, and other standards for corporate governance, will realize the benefits of a proven solution for corporate governance. Therefore, policy enforcement starts at the top of the pyramid.

The practicality of any security policy depends on whether that policy is enforceable and at what cost [16]. Users cannot always see what effect a policy might directly have on them. The ability of the end-user of an organization to understand its policy is important to ensuring that the policy is followed. It is argued [3] that effective policy enforcement involves assuring that the policies are understood by all users, and having well-defined procedures to deal with incidents of policy violation.

Effective policy enforcement involves several elements and the policies need to be implemented in multiple ways: Monitoring, documenting, training, implementing enforcement technologies, and others. Organizations must have a unified way of enforcing policies in different products that the organization acquires.

### 5.1 Monitoring of the Working Environment

Constant monitoring of the working environment, the configuration, and the network to ensure that violations have not occurred is the first step in enforcing policies. Constantly monitoring the configuration of computers is a valuable practice to identify breaches of security. A computer may be infected or suddenly out of compliance at any time it is connected to the network. For instance, consider using a policy enforcement system to isolate computers from the network if its antivirus application isn't running [21].

### 5.2 Documenting All Security Incidents

While documenting all security incidents, organizations also need to document the methods used to detect and deal with security violation. Part of the monitoring of the work environment should be on generating reports and possible trends in security violations and analyzing trends of security related issues.

### 5.3 Implementing Enforcement Technologies

Policy enforcement technologies extend the familiar notion of granular access control beyond user and machine identity, into the endpoint computer's configuration and network environment. This capability for enhanced examination of a target machine is generally implemented through a proprietary software agent [21]. For instance, implementing a data loss prevention product when sending an e-mail, the product will check the policy and it would require approval before allowing data to be sent in an email. Another application may be implemented to allow you not to copy data into removable media.

Enforcement technologies exist from many vendors. The Trusted Computing Group has created an open architecture for endpoint integrity. The architecture enables network operators to enforce policies regarding endpoint integrity at or after network connection. This standard architecture ensures multi-vendor interoperability across a wide variety of endpoints, network technologies, and policies [22]. Other products are available from different vendors such as: Cisco Network Admission Control [23], Microsoft Network Access Protection [24], Endpoint Security Mailing List, and others.

Cisco Network Admission Control (NAC) enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be on the basis of information about the endpoint device, such as its current antivirus state. It allows noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network. The decision is made based on a policy that exists on Cisco Secure Access Control Server [23].

Microsoft Network Access Protection (NAP) solution enforces the policy by constant monitoring and assessing the health of client computers when they attempt to connect or communicate on a network. Computers that are not in compliance with the policy can be provided with restricted network access until their configuration is updated and brought into compliance with the policy. Noncompliant computers can be quarantined or automatically updated so that users can quickly regain full network access without manually updating or reconfiguring their computers [24].

### 5.4 User Training

Training continues to have a significant organizational impact. End-user training takes the largest portion (38.4%) and it deals with the teaching of skills to effectively use computer applications [12]. Training and user education should focus on procedural issues rather than effective use of computer applications. A procedural attack takes the form of a social engineering attack. It is argued by [25] that a social engineering attack manipulates people into performing actions or giving confidential information. While [26] argues that an appearance of authority may be interpreted as having actual authority in social engineering attacks. The study in [26] also supports the concept that understanding of the value of information as well as proper usage of information is as important as an awareness of social engineering efforts.

It is typical for organizations to mandate that users declare and acknowledge receiving the information security policy. In signing a user declaration upon employment before access to electronic information is granted, the user acknowledges his/her responsibility with regard to information security. A user should know his individual responsibilities in protecting information assets within his organization [15]. One way to ensure that users know their responsibilities in protecting the organization is by training them on how to protect the organization.

Enforcement technologies make enforcement possible for physical and computer security. But for protecting the organization from the vulnerabilities of its users, it requires more than an automated system. Social engineering attacks bypass the enforcement technology by attacking the weakest link, the users. Such attacks according to [27] can occur on both a physical and psychological level. The physical setting for these attacks occurs where a victim feels secure: often the workplace, the phone, even around the water cooler. Psychology is often used to create a rushed situation that helps the social engineer to get information about accessing the system from an employee. In both cases the attack is possible due to inadequate education of the users.

## 1. CONCLUSION AND CONTRIBUTION

It is clear that the three dimensions of security are of a non-technical nature. All these dimensions must be taken into account in designing and creating a comprehensive information security plan for organizations, because no single dimension, or product or tool on its own will provide a proper all inclusive solution. While it is the responsibility of organizations to provide physical and computer security, organizations should take responsibility in providing training and education in security related issues and against social engineering attacks. This type of attack is preventable by training and educating users of the threats.

The topics of users, policies, and enforcement have received a fair amount of research attention but each part was viewed in isolation of the other two complementary parts. Both the users and security policy are important factors for organizations to fulfill the goals and objectives. Although the goal of automating the enforcement of security policy from higher-level objectives remains worthy, it is not practical for all but the most trivial scenarios. However, this does not preclude that partial automation of the enforcement by using tools that can assist users is

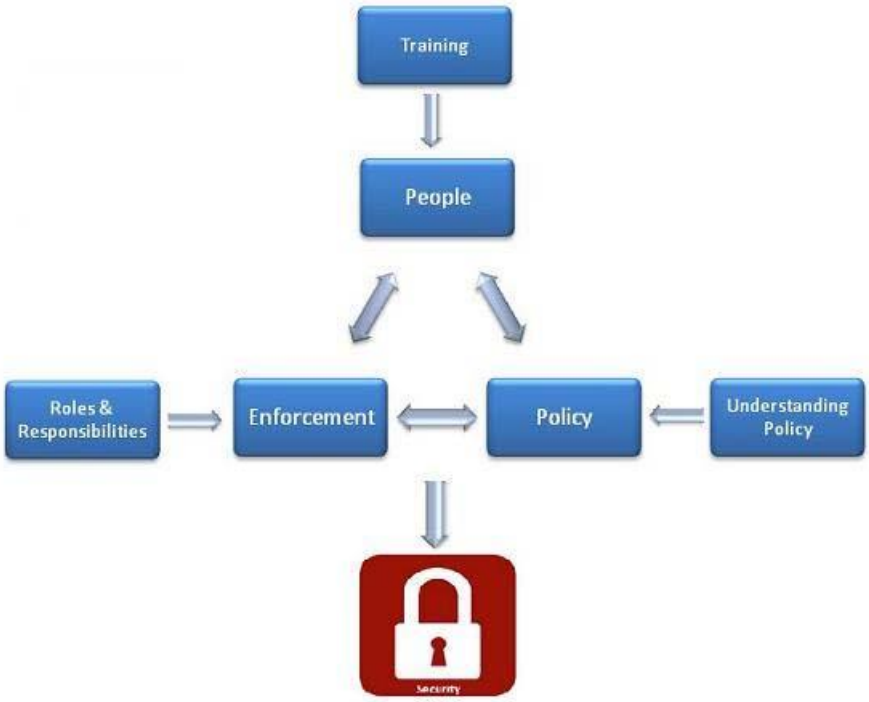
not needed.

In the security and audit community each part has received a fair amount of research attention and the most promising approach seems to investigate the requirements and relies on identifying, recognizing, and instantiating refinement patterns. While a much simpler approach of integrating the users with policies is described in detail. It is desirable to maintain the properties of consistency and completeness when refining and enforcing policies.

Users are often the weakest link in an otherwise secure organization and, consequently, are targeted by social engineering attacks. The only protection against social engineering attacks is to educate the users. A discovery and disclosure approach should be followed. The disclosure should provide users with a sense of security that raises their awareness of the threats that their information systems face. Organizations are more interested in long-term effects of training and the areas of end-user learning, rather than training. Organizations want the training to be transferred to the workplace. Signing and acknowledging the receipt of an information security policy should be after educating and training the users. The user declaration and acknowledgement should also be read and signed again on an annual basis.

We provided evidence for writing policies that can be implemented. Implementation requires understanding of those policies by the users. A formal security policy is a prerequisite of security. Vague policies will increase the occurrence of non-compliance. Therefore, the security policy should inform the end-users of their roles and responsibilities in protecting the organizational assets. Organizations should enforce policies in a unified way. The ability of the end-user of an organization to understand its policy is important to ensuring that the policy is followed. Effective policy enforcement involves assuring that the policies are understood by all users, and having well-defined procedure to deal with incidents of policy violation.

**Figure 3: Model for the three dimensions of security**




The basis for a formal policy-to-enforcement was shown to consist of:

. Constant monitoring of the working environment, the configuration, and the network to ensure that violations have not occurred is the first step in enforcing policies.

.
. Analyzing possible trends in security violations and analyzing trends of security related issues.
. Implementing enforcement technologies
. Training in security related issues will have a significant organizational impact

This conceptual framework combined the users, the policies and the enforcement into a solution that transformed the users from being the weakest link, the enemy within, in an organization into responsible users who play a role in organization security. This role begins with training the users in security related issues and participants in writing security policies. This role ends in users enforcing policies and transforming organization into secure ones (see Fig. 3)

## 1. FUTURE WORK

For the future work, we propose tracking the usage of social networking websites like Facebook and Twitter in aiding social engineering attacks. A social engineering attack gathers information about users before performing actions against an organization.

In addition to social engineering attacks, we propose protecting the configuration systems. It is also desirable to encrypting the exchange of messages between systems to avoid eavesdropping. Many systems implement automatic updates that require downloading and installing new software. Many implementations are implemented without the users being involved. An investigation that compares automatic updates versus manual updates by the users will be carried out.

## 1. REFERENCES


1. Saleh, M.F., *Information Security Maturity Model* International Journal of Computer Science and Security (IJCSS), 2011. **5**(3): p. 21.
2. David, J., *Policy enforcement in the workplace.* Computers & Security, 2002. **21**(6): p. 506-513.
3. Madigan, E.M., C. Petrulich, and K. Motuk, *The cost of non-compliance: when policies fail*, in *Proceedings of the 32nd annual ACM SIGUCCS fall conference*. 2004, ACM: Baltimore, MD, USA. p. 47-51.
4. Norman, D.A., *The Way I See it: When security gets in the way.* interactions, 2009. **16**(6): p. 60-63.
5. Vidyaraman, S., M. Chandrasekaran, and S. Upadhyaya, *Position: the user is the enemy*, in *Proceedings of the 2007 Workshop on New Security Paradigms*. 2008, ACM: New Hampshire. p. 75-80.
6. Schneier, B., *Secrets and Lies: Digital Security in a Networked World*. 2000, New York: John Wiley & Sons, Inc.
7. Corporation, M. *The Enemy Within*. 2005 [cited June 20; Available from: http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/.
8. Adams, A. and M.A. Sasse, *Users are not the enemy.* Communications of the ACM, 1999. **42**(12).
9. Gross, J. and M.B. Rosson. *Looking for Trouble: Understanding End-User Security Management*. in *Computer Human Interaction for the Management of Information Technology (CHIMIT)* 2007.
10. Sasse, M.A., S. Brostoff, and D. Weirich, *Transforming the 'Weakest Link' - a Human/Computer Interaction Approach to Usable and Effective Security.* BT Technology Journal, 2001. **19**(3): p. 122-131.
11. Kumaraguru, P., et al., *Teaching Johnny not to fall for phish.* ACM Trans. Internet Technol., 2010. **10**(2): p. 1-31.
12. Gupta, S., R.P. Bostrom, and M. Huber, *End-user training methods: what we know, need to know.* SIGMIS Database, 2010. **41**(4): p. 9-39.
13. Compeau, D., et al., *End-user training and learning.* Commun. ACM, 1995. **38**(7): p. 24-26.
14. McCoy, C. and R.T. Fowler, *"You are the key to security": establishing a successful security awareness program*, in *Proceedings of the 32nd annual ACM SIGUCCS fall conference*. 2004, ACM: Baltimore, MD, USA. p. 346-349.
15. Höne, K. and J.H.P. Eloff, *Information security policy what do international information security standards say?* Computers & Security, 2002. **21**(5): p. 402-409
16. Schneider, F.B., *Enforceable security policies.* ACM Transactions on Information and System Security, 2000. **3**(1): p. 30-50.
17. Craig, J.S., *The human element: training, awareness, and human resources implications of health information security policy under the Health Insurance Portability and Accountability Act (HIPAA)*, in *2009 Information Security Curriculum Development Conference*. 2009, ACM: Kennesaw, Georgia. p. 95-99.
18. Johnson, M., et al., *Optimizing a policy authoring framework for security and privacy policies*, in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 2010, ACM: Redmond, Washington. p. 1-9.

19. Hall, D.E., *Requirements and policy challenges in highly secure environments*, in *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*. 2004, ACM: Paris, France. p. 897-898.
20. Solmsa, B.v. and R.v. Solms, *The 10 deadly sins of information security management.* Computers & Security, 2004. **23**: p. 371-376.
21. Bird, T. *What is policy enforcement, and why should we care?* 2004; Available from: http://www.computerworld.com/s/article/98080/What_is_policy_enforcement_and_why_should_we_care_?taxonomyId=17&pageNumber=3.
22. Group, T.C. *Trusted Network Connect*. 2010 [cited 2011 June 28]; Available from: http://www.trustedcomputinggroup.org/developers/trusted_network_connect/.
23. Cisco. *Network Admission Control.* 2011 [cited 2011 June 28]; Available from: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html.
24. Microsoft. *Network Access Protection*. 2011 [cited 2011 June 28]; Available from: http://www.microsoft.com/windowsserver2008/en/us/nap-main.aspx.
25. Robling, G. and M. Muller, *Social engineering: a serious underestimated problem.* SIGCSE Bull., 2009. **41**(3): p. 384-384.
26. Kvedar, D., M. Nettis, and S.P. Fulton, *The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition.* J. Comput. Small Coll., 2010. **26**(2): p. 80-87.
27. Orgill, G.L., et al., *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*, in *Proceedings of the 5th conference on Information technology education*. 2004, ACM: Salt Lake City, UT, USA. p. 177-181.