
Nadianatra Musa¹, Rosita Mohamed Othman², Dayang Hanani Abang Ibrahim³, Inson Din⁴
Faculty of Computer Science and Information Technology (FCSIT)
Universiti Malaysia Sarawak (UNIMAS)
Kota Samarahan, Sarawak, Malaysia

Abstract—The increasing use of E-Government Services applications has created a lot of opportunities by fraudsters to commit E-Fraud crimes from remote locations. The rise of E-Commerce frauds has significant impact over E-Government services applications. Maintaining community confidence and developing trust to its citizen are seen as the key challenges by government agencies in order to sustain its credibility and competitive advantage. Therefore, E-Fraud and perpetrator platforms employed by fraudsters are explored to review techniques/methods used by them. The security problem including E-Fraud cannot be solved using a linear approach (narrow approach) because E-fraud is a complex and requires concurrent interaction from other components. In this study, E-Fraud prevention for government agency is proposed and classified into three components first, the formal component, second is the technical component and third is informal component.

Keywords- E-Fraud; E-Government Services, Formal component, Technical component, Informal component, Information Security

I. INTRODUCTION

The greater diffusion and decentralization of E-Government Services throughout the Government Agencies have also increased the risks that associated with Information Systems and Information Technology. The increasing use of E-Government Services applications has created a lot of opportunities by fraudsters to commit E-Fraud crimes from remote locations such as office networks, office buildings, Hot Spots locations (e.g. Cafes), airports lounge, Wifi services, unsecured wireless services and etc. It was identified there are two types of fraudsters, first is those who are internal employees and second is those who are external people to government agency. The risks relating to E-Fraud may come from human actions either intended (e.g. social engineering attacks) or not intended (e.g. ignorance, stupidity), technical deficiencies (e.g. bugs, errors) and insufficient of formal procedures (e.g. unclear roles and responsibilities) of an organization.

Very recently, the incident of cybercrimes in Malaysia rose by 88 per cent in 2011 from 8,090 in 2010 to 15,218 cases in 2011 within the government agencies [1]. It is presumed the number of E-Fraud will increase dramatically if there were no effective and efficient security controls within organization. The major focuses of Government Agencies are to maintaining community confidence and developing trust to its citizens with the security of the information held. More importantly from the citizen's perspective, government is seen as one entity, where if a security problem occurs within one government agency is also reflected to the whole of government process. Therefore, continuity of improving security is viewed as vital by government agencies to protect itself and its citizens particularly. This paper is divided into five sections. After a brief introduction, the next section discusses the E-Fraud in terms of information security over the E-Government Services applications. Then, the third section describes the perpetration platforms used for fraudulent activities. Section four develops a conceptual framework of the E-Fraud prevention for government agency and finally the last section summarizes up the paper contents.

II. E-FRAUD OVER E-GOVERNMENT SERVICES

From the perspective of government, fraud according to the Commonwealth of Australia is described as “inducing a course of action by deceit or dishonest conduct, involving acts of omissions or the making of false statements, orally or in writing, with the object of obtaining money or other benefit from, or evading a liability to the Commonwealth” [2]. In the Dictionary of Law, fraud is defined as “1. wrongful or criminal deception intended to result in Financial or personal gain or 2. a person or thing intended to deceive.” [3]. Internet Fraud Complaint Centre (IFCC) uses the notation Internet fraud for fraud committed over the Internet [4]. There are nine categories of E-Fraud crimes towards the various electronic applications complaints received and reported on the cyberspace. The categories are confidence fraud (e.g. non delivery fraud), financial institution fraud, gaming fraud, business fraud, investment fraud, communication fraud, insurance fraud, utility fraud and government fraud. Hence, government fraud is a fraud against the government in order to get some benefit. This category includes tax evasion when the tax forms are filled out online [4].

It can be seen that all examples of nine categories of E-Fraud crimes are indicating the cyberspace world would lost control over its territory and would unable providing the most basic service to its citizens if not properly controlled.
and monitored. Recently, [3] claims cyberspace is a failed state as it has also borders, currency, laws and citizens.

By looking at how the term E-Fraud is used today, it is hard to define what E-Fraud is. There is no general definition of E-Fraud. After going through various literatures, the following definition best describes what E-Fraud is,

“E-Fraud is defined as a deception deliberately practiced to secure unfair or unlawful gain where some part of the communication between the victim and the fraudster is via a computer network and/or some action of the victim and/or the fraudster is performed on a computer network.”[5].

E-Government Services are an application to make government to citizen (G2C) transactions more efficient, effective and productive, while enhancing the quality of services, by facilitating public transactions with government using various electronic channels [6]. From the E-Government Services definition that given by [6], citizens perceive the cyberspace is a new territory, which may improve their social value in their continuing life. However, getting citizenship on the cyber space would be a nightmare to certain people as it is vulnerable to E-Fraud crimes.

E-fraud cases indeed have a significant impact over E-Government Services as cyber world purposely opened to all. Since the era of Internet, cases involving e-fraud on the government services applications have been on the rise in Malaysia. As reported by [1], the majority cases were by E-Fraud with 5328 cases, followed by the intrusion or attempted intrusion with 4,439 and not much on cyber harassment with only 459 cases.

To date, even though Malaysia passed four cyber laws which comprises Computer Crimes Act, Digital Signatures Act, the Copyright (Amendment) and Telemedicine Act (1997), but the number of fraudulent activities is overwhelmingly increased from time to time. Currently, in Malaysia, Internet World Stats estimates the number of Internet users in Malaysia at 17,723,000 in 2011 which represents about 1.7% of Asia’s Internet users, with a penetration rate of 61.78% and it was recorded about two-third (68%) of the Malaysian Internet users registered and joined the social networking-Facebook [7]. As the number of cyber space citizens grows rapidly, the possibility of E-Fraud crimes would also raise eventually.

E-Fraud in fact jeopardizes the citizens of E-Government in terms of money losses. It can cause instability in a system and indeed impose a very significant cost on society [8]. For example, Table 1 shows the top 10 of Internet Scam Trends from National Consumers League (NCL) Fraud Center for the year of 2007 reporting on the category of Scam and its average loss [9]. The study [9] identified two categories which were ‘Fake Check Scams’ and ‘General Merchandise’, have received major complaints from consumers.

<table>
<thead>
<tr>
<th>Category</th>
<th>% of all complaints</th>
<th>Average Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fake Check Scams</td>
<td>29%</td>
<td>$3,310.87</td>
</tr>
<tr>
<td>Consumers paid with phony checks for work or items sold, instructed to wire money back</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Merchandise</td>
<td>23%</td>
<td>$1,156.84</td>
</tr>
<tr>
<td>Sales (not through auctions), goods never delivered or misrepresented</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorizes*</td>
<td>13%</td>
<td>$1,371.08</td>
</tr>
<tr>
<td>Goods never delivered or misrepresented</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nigerian Money Offers</td>
<td>11%</td>
<td>$4,045.14</td>
</tr>
<tr>
<td>False promises of riches if consumers pay to transfer money to their bank accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lotteries/Lottery Clubs</td>
<td>7%</td>
<td>$998.43</td>
</tr>
<tr>
<td>Requests for payment to claim lottery winnings or get help to win, often foreign lotteries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advance Fee Loans</td>
<td>3%</td>
<td>$1,510.77</td>
</tr>
<tr>
<td>False promises of business or personal loans, even if credit is bad, for a fee upfront</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prizes/Sweepstakes</td>
<td>3%</td>
<td>$1,181.58</td>
</tr>
<tr>
<td>Requests for payment to claim prizes that never materialize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>3%</td>
<td>$220.47</td>
</tr>
<tr>
<td>Emails pretending to be from a well-known source, asking to confirm personal information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friendship and Sweetheart Scamming</td>
<td>1%</td>
<td>$3,038.31</td>
</tr>
<tr>
<td>Con artist maintains an online relationship, convinces victim to send money</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Access Services</td>
<td>1%</td>
<td>$896.99</td>
</tr>
<tr>
<td>Cost of Internet access and other services misrepresented or services never provided</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* In the fall of 2009, online gift cards were the hot item in Web use fraud.org. As a result, the number of fraud complaints reported to NCL’s fraud center has dropped to a fraction of its previous levels.

To have a better understanding of E-Fraud the Government Agencies threat is, consider the E-Fraud cases in the public sectors, the following cases were presented by [10] as follows.

• In Australia, Electronic Benefits Transfer (EBT) systems are being used for the delivery of social security benefits, however these have been misused. Authorized recipients can use plastic cards to obtain cash from ATMs. In Australia a number of prosecutions have taken place in respect of internal fraud carried out by government employees fraudulently using the EBT computer system in December 1997 and January 1998. EBT cards were issued in fictitious names enabling the offenders to obtain cash at ATMs. In one case reported by Warton (1999), the proceeds of the fraud were used to purchase heroin in the same street as the location of the ATM and within 10 minutes of the fraud occurring.

• Another case example of E-Fraud occurs in the E-Procurement services. Electronic procurement, however, carries risks of fraud and abuse as internal controls may be removed when new electronic procurement systems are introduced. Government agencies are particularly vulnerable in view of the extensive procurement activities in which they engage and the large sums of money involved. In one Australian case, for example, Bell (2000) presented an evidence, a sub-contractor to a local Council in New South Wales allegedly gained access to the Council’s database of tendering information.
and was able to secure numerous contracts through the use of this information. [10]

From the cases reviewed in the earlier paragraph, the protection of information over e-government services applications is critical as government agencies collect and use vast amounts of citizen’s information to services to people and serving the community.

Apart from providing services to citizens of E-Government, the security of the information is crucial to maintaining citizens’ confidence with E-Government Services. Information security is about integrity, confidentiality, availability [11] and non-repudiation [12]. Integrity must protect information from modification or alteration from unauthorized subjects, confidentiality must protect information from improper disclosure and availability must make information available when required by authorized subjects. As many of e-services take place on the cyberspace, non-repudiation ensures one cannot denies an action of signing a contract in particular trading or contracts. If one of those security elements were compromised, it would lead to the creation a lot of unexpected crimes activities. The most common of E-Fraud case is credit or debit card fraud. This fraud is where someone uses stolen credit or debit card numbers to buy goods or services online and namely as impersonation.

As in E-Government Service transactions, the Government has to be able to demonstrate confidentiality, competence and integrity in handling a person's data, and therefore has to inspire trust. Various points are put forward on whom members of the public have to be able to trust the Government's eServices. These fell into three broad areas, which are first is the service working correctly and efficiently, second is the information only being used for the intended purpose and third is data being held securely against malicious attack [13].

After reviewing the E-Fraud on E-Government services, it might be useful to look the perpetration platforms used by fraudsters to commit the fraudulent activities.

III. PERPETRATION PLATFORMS OF FRAUDULENT ACTIVITIES

E-Fraud is the use of electronic platforms by perpetrators to commit fraudulent activities. Taxonomy of computer fraud by Vasiu & Vasiu [14] defines perpetration platforms as With or Without Authorization.

The first class of perpetration platform is With Authorization. This defines a legitimate user that exceeds the authorized access. The fraud crimes are always committed by internal threats, especially senior employees because they may have greater access to assets in the organizations for their own benefits [15]. As identified by [14], one case in US where fraud crimes are committed by accountants, where they pled guilty to exceeding their authorized access to the computer systems of Cisco System in order to illegally issue almost $8 million in Cisco stock to themselves. In dealing with this ethical issue, government agencies might consider this type of platform class is a serious threat against e-government services application.

However, the second perpetration platform is Without Authorization. The Without Authorization is the act of accessing a protected application that is not approved by the system owner or administrator. Perpetration platforms of computer fraud taxonomy by Vasiu & Vasiu [14] are referred and extended in the context of e-government world. The Without Authorization is subdivided into masquerade and vulnerability exploitation. Masquerade is the unauthorized impersonation of an authorized user or of an entity. Under this category there are two types of masquerade, first is spoofing attacks and second is impersonation. Whilst, the second type of without authorization, which is vulnerability exploitation, might involve a combination of vulnerabilities such as software bugs, error of omission, incompetence, administration errors and failure of Internet access control system.

Understanding the types of platforms (With or Without Authorization) would help the government agency to strategically deter and prevent from any deliberate or non-deliberate actions such as human error, integrity of people and technological issues.

The next section will develop a conceptual framework of formal, technical and informal components of E-Fraud prevention and background and provide some solutions employed by various organizations to prevent E-Fraud from technological solutions to non-technological solutions.

IV. A CONCEPTUAL FRAMEWORK: THE FORMAL, TECHNICAL AND INFORMAL COMPONENTS OF E-FRAUD PREVENTION

A. The Three Components of E-Fraud Prevention

In reality, E-Fraud maybe detected in many cases, however, prevention is better than cure. Early detection can contribute to fraud prevention. The organizations may perform some security activities to protect its critical business data, employees data and customer information from being manipulated and impersonated by fraudsters. This section will discuss how the three components of formal, technical and informal could address the E-Fraud issues in the government agencies, see Figure 1. First is prevention through formal component, second is prevention through technological component and third is prevention through informal component. The non-technological solutions such as formal and informal components are considered as soft measures and technological are considered as hard measures [16].

![Figure 1. The three components of E-Fraud Prevention](image)

Formal components

Technical component

Informal component
i. Formal Component

Not much IS/IT security researchers focus on formal components such as IS/IT security vision, the alignment between business and IS/IT security, IS/IT security standards, IS/IT security policies, procedures and laws/regulation. The IS/IT security research is primarily dominated by the technological and computational solutions [17-19]. For instance, [9] highlighted many security researchers using mathematical approaches to prevent any type of IS/IT risks.

However, a security planning model by [20] shows that formal components such as security policies are critically needed to deter employees from committing intended or unintended actions within the use of IS/IT. There are four sequential stages of security actions for managing system risks, first is deterrence, second is prevention, third is detection and fourth is recovery [20]. IS/IT security policy, security awareness programs and guidelines are the examples of deterrence activity, the deterrence countermeasures do not require enforcement but depending on the willingness of IS/IT users to comply. This kind of viewpoint indirectly influences the organizational stance about managerial role in the effective implementation of information security policy and procedures. Information security is no longer the concern of Chief Information Officer (CIO) or Chief Security Officer (CSO), but also the concern of all other line managers [18,21]. All line managers of each division are increasingly involved in information security issues [22].

Information security policy is the heart of the organization [23]. With no policies, there will be no procedures or countermeasures in engaging security issues at organizational level. Information security policy is the most important control needed by organization to manage the implementation and the effectiveness of information security practices [24].

ii. Technical Component

The Technical component may vary ranging from hardware, network to software approaches. There are many security controls and countermeasures can be employed by government agency to minimize risk relating to IS/IT especially E-Fraud activities. For example, Secure Socket Layer (SSL) can be used to protect sensitive information, firewalls can be used to protect internal networks and data storages, virus scanning software can be used to protect against viruses, security patches should be used to update used software. Other technical solutions including 3D-model based solutions, SET and EMV smart cards, complemented by a real time authorization by the issuer, address and CVV/CVC2 validation, the use of passwords and user IDs, virtual and pseudo card numbers. Apart from that, the security of technology infrastructure of the consumers, merchants, banks and service providers needs to be taken into consideration as online transactions take place. The advanced and secured payment schemes are critical to foster the high information security standards deployed by banks, merchants and service providers. The aim of those solutions are clearly aiming to provide network security [25], data confidentiality, data integrity, consumer and merchant authentication and non repudiation for each individual transaction [16].

iii. Informal Component

The other type of non-technological solutions is Informal component. Informal components are referred to employee values, culture and norms of the organization. The strongest factor in information security is not technology but the people [26]. Human value is a non-technology based factor, which needs special attention because human maybe the weakest link in securing information systems and they have an access to system and very sensitive information. Security incidents that involve internal user such as employees, particularly at management level [27] happen more frequently than attacks from people outside the organization. This is because of opportunities are presented though lax security [28]. Even though the Policies and Codes of Ethics are in place, but it is not enough to manage E-Fraud alone as these policies or codes have its limitations. For example, in his [29] study comparing laws and code of ethics, he reported codes of ethics do have an effect, but they are related only to certain abuses. The codes of ethics do not necessarily make a person behave ethically [29]. Some of the non-technological solutions have been implemented to reduce E-Fraud among different actors (users or consumers, merchants, organizations and service providers) are awareness of security risks at all organizational levels, education of employees, merchants, consumers and end-users, good internal security managerial, organizational and operational policies and procedures, screening and monitoring of employees, screening fraudulent transactions and invest in professional security review [30].

The security culture that exists in the organization may contribute to the effective of IS/IT implementation. The top management of government agency has responsibility in the cultivation of security culture through policies, guidelines, standards or other controls/countermeasures. Information security policy implementation should reflect in hand with organization’s culture and management commitment [24,31,32]. In health care environment, [31] has argued that security policy with practical procedures can be achieved effectively and indirectly through some collaboration and commitment from senior management and strong leadership from within health care professions. Hone & Eloff [24] have admitted the role of management’s commitment in information security policy is important in realizing the firm’s vision and mission. Yet several others perspectives warn that culturing information security policy can only be achieved through proper education process [32-34].

B. Relationship between the three components and its scenarios

The interactions between the three components of formal, technical and informal are crucially needed by government agencies to retain competitive in cyberspace world. In Figure
2, the implementation of a particular component should be aligned with another component(s) because security problem such as E-Fraud is not merely a technical problem but also a social problem [35]. Like other industries, E-Government Services must ensure the IT infrastructures are safe, conducive and credible environment. To achieve this environment, there are two types of contexts that needed to be taken into consideration, the External context and the Internal context. In the conceptual framework developed in Figure 2, the E-Fraud Prevention considers the elements from two contexts, first is an External context and second is an Internal context. The External context is concerned with external elements/forces coming from outside of the government agency such as regulation, international standard, industry guidelines and ethics/professional bodies. The Internal context is associated with elements that exclusively exercised by the top management such as vision, policies, technical procedures, culture and employee values. Both types of contexts are important for handling E-Fraud because security problem is a complex and not linear, this conceptual framework exploring the dynamic of component interaction between the formal, technical and informal components.

The applications of component interactions are presented in the following examples and a scenario.

i. The interaction between Informal and Formal Components

The Informal components like security culture and employee values have an interaction with the Formal component like policies. For instance, in the case of the Arthur Andersen/ Enron, the information security incident was the result of lack of people’s integrity but not the matter of good policy [32].

ii. The interaction between Formal and Informal Components

The implementation of formal component could be affected by the Informal component. To achieve the interaction between two components, the management must ensure the creation of policies is not infringing any individual’s personal assumptions and beliefs, norms, collective values and knowledge [33].

iii. The interaction between Formal, Technical and Informal Components

Consider the following scenario and understand how the component interaction between formal, technical and informal components can be applied in the following problem.

Problem: An ABZ government agency found out their accountant had committed E-Fraud, the Audit committee examined and detected some deficiencies and inconsistencies over the financial reported on the Accounting Information System.

Analysis: Using the E-Fraud prevention as shown in Figure 1, it has been found that the ABZ government agency had a proper organizational structure and policies for information security. To achieve the business goals, this government agency had adopted information systems including Accounting Information System and Human Resource Management System which are in-lined with policies. However, the policies relating to the use of databases for Accounting Information System did not specify the security privileges among the IT users. This deficiency has exposed the databases of the government agency to potential perpetrators to commit fraudulent activities in the organization. The legitimate users may exceed the authorized access or fraudulent activity due to:

- the access controls of database management system such as Mandatory Access Controls and Discretionary Access Controls were not clearly defined in the IS/IT policies (Formal). The government agency should ensure the computer users are defined according to their roles and designation where a user at a given security level may not read an object at a higher security level. If these elements have been defined, investigate other components.
- irrelevant adoption of security controls and security countermeasures may risk the government agency because the security requirements were not aligned with the business goals. The examples of risks from the misalignment are loss of business data/secrecy information, damage of reputation and financial loss/low Return of Investment. Another reason would be the government agency does not have effective security controls in place to detect and automatically stop the suspicious activity from happening (Technical).
- if the policies relating to Access Controls were already in place, but the fraudulent activities still occur, the government agency needs to identify whether or not the employees have been trained with related skills. If the employee has been trained, it is no longer policy issue but social issue such as lack of integrity and lack of honesty. Then the government agency has to adopt the recovery approach where employees should be given reprimands, warnings, resuffle or termination in order to avoid accepting risk.
Figure 2. A conceptual framework of E-Fraud Prevention for Government Agency: The three components of formal, technical and informal components

V. CONCLUSION

The paper has revealed the incidents of E-Fraud and its impacts through findings and statistics from various credible organizations. The E-Fraud definitions have been referred and applied within the context of E-Government Services domain. Importantly, E-Fraud cases have given us some indications the importance of information system security. System instability and monetary losses on society are seen as some of the E-Fraud impacts. There are two types of perpetrator platforms discussed which are With Authorization and Without Authorization. Whilst, in terms of E-Fraud prevention, the paper has grouped prevention into three types of components, first is from formal component, second is from technical component and third is from informal component. The conceptual framework of E-Fraud Prevention is illustrated using few examples and typical scenario of government agency. The study has also presented the concurrent interaction between three components is complex, in fact E-Fraud is not only technical and management problems but also a social problem.

REFERENCES


