OSJ OPEN SCIENCE JOURNAL

CASE REPORT

E-commerce risk management: analysing the case Vietnam Airlines incident

Chu Ba Quyet[1]*, Hoang Cao Cuong[1]

[1]Thuongmai University, Vietnam

*Corresponding author: Chu Ba Quyet: quyetcb@tmu.edu.vn

OPEN ACCESS

Citation: Qyuyet C.B., Cuong H.C. (2017) E-commerce risk management:analyzing the case of Vietnam Airlines incident. Open Science Journal 2(4)

Received: 21st July 2017

Accepted: 12th September 2017

Published: 6th November 2017

Funding: The author(s) received no specific funding for this work

Competing Interests: The author have declared that no competing interests exists.

Abstract:

E-Commerce is the purchase and sale of goods, services and exchange of information based on communications networks and the Internet. Information, information systems, computers, computer networks, and other electronic means play an especially important role. These objects are valuable assets and targeted attacks by cybercriminals. E-commerce risk management is to protect the development of e-commerce. It includes setting information security objectives, assessing vulnerabilities, threats and attacks, and selecting countermeasures. The paper presents the theory of e-commerce risk management, analysing the Vietnam Airlines e-commerce risk management case, using the DREAD model. The paper provides the discussions and short recommendations to other enterprises in e-commerce risk management nowadays.

Keywords: Social Work, Effectiveness Evaluation, Practice Improvement, Substance Abusers, Peer Support

Introduction

E-Commerce brings a lot of opportunities for organizations and consumer in nowadays. As a result, more and more Vietnamese businesses are using eCommerce, building information systems, designing websites to sell goods, and providing online services. However, e-commerce boom has also generated chances for cybercriminals to develop. Although the e-commerce development in Vietnam about more than ten years, but many enterprises has not experienced in managing e-commerce risk. The paper presents some theories of e-commerce risk management, analysing Vietnam Airlines (VNA) incident in 2016, and discusses how to managed eommerce risk by VNA in practice.

Literature Review

Ecommerce risk

In short, risk is a situation involving exposure to danger. Businessdictionary defines: “Risk is a probability or threat of a damage, injury, liability, loss, or other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action”. A risk is not an uncertainty. Risk is the potential of gaining or losing something of value. Risk can also be defined as the intentional interaction with uncertainty [9]. Risks can be seen as relating to the probability of uncertain future events, the probable frequency and probable magnitude of future loss.

In information security, risk is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization [5].

E-commerce risk or risk associated with eCcommerce is a typical risk in information security. There are many types of e-commerce risks. This study presents e-commerce risks from an information security perspective. It happens when the e-commerce information system is likely to become unsafe, the cause may be due to an incident: hacked, exploited vulnerabilities ... and resulting in losses as disclosure of information, does not meet the requirements of immediate retrieval, incorrection or deletion of information, caused to the user or owner to suffer damages or losses.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [10]. Information security is the guarantee, confidentiality, integrity, and availability of information. According to ISO / IEC 27000: 2009, it can include: authenticity, accountability, denial and reliability. Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to ensure the reliability, integrity and availability of information (CNSS, 2010). "Information security is to ensure that only competent persons have access to complete and accurate information when needed." (ISACA, 2008). Many organizations defined the term of information security. In general, information security includes the following requirements (see table 1)

Table 1. Information security requirements

Requirement	***Definition***
Confidentiality	*means that information is not disclosed to unauthorized or leaked objects*
Integrity	*means the data is not modified*
Availability	*information must be available when needed*
Denial	*It means that a party can not deny that they have dealings with other parties*
Authenticity	*to ensure that stakeholders know who they are in the system; and*
Privacy	*the ability to control the use of personal information provided by customers about themselves*

E-commerce is trade based information. If the transmitted information does not fulfil the requirements for availability, integrity, disclosure..., the parties may suffer losses. Therefore, e-commerce risk is the type of information risk related to the information and e-commerce systems are harmed and unsafe. This relatively new term was developed as a result of an increasing awareness that the information security issue is the cause of a many of eCommerce risks that are relevant to IT. The cause is that these systems are compromised, attacked by the exploit of system vulnerabilities.

There are many sources of e-commerce risk, such as computer crime, spyware, malware, adware, spyware, computer worms and computer viruses. The origin of e-commerce risk is the threat or dangerous sources, the opposing forces that can affect e-commerce transactions.

The essence of e-commerce risk is the potential loss from the threat or an attack of exploiting a vulnerability. Risks are generated as a result of one or more security attacks exploiting vulnerabilities to compromise information or e-commerce system targets. As such, there may be one or several threats, but if there is no hole or no flaw, there is no information risk existence. Similarly, e-commerce systems are experiencing vulnerabilities, but if there are no exploits that exploit vulnerabilities or vulnerabilities have been patched, then there may be no risk. Briefly, risk is the intersection of ecommerce assets, threats or attacks, and vulnerabilities (see Figure 1).

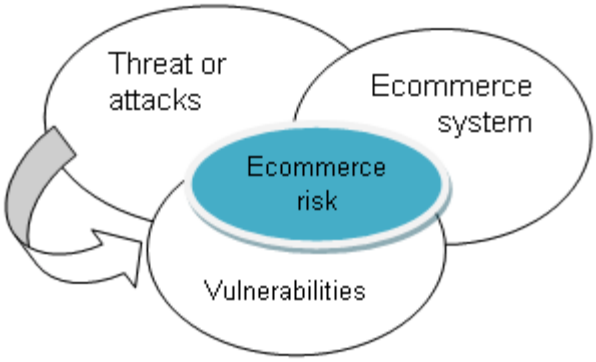

Figure 1. Ecommerce risk essence
Source: Authors

In many cases, threats and attacks and vulnerabilities are often closed or tied to each other [3]. Therefore, detecting or discovering the type of vulnerability can also help to anticipate the type and severity of threat or type of attack. Whenever, the detection of vulnerability is always a top priority in managing information risk or ecommerce risk.

Ecommerce risk management

Risk management is the identification, assessment, and prioritization of risks. It followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities [4]. Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals. In

eCommerce, risk management is the process of setting goals and targets for protection, analyzing threats or security attacks and exploiting vulnerabilities, assessing and ranking risk levels, and selecting countermeasures in eCommerce enterprises or any eCommerce project.

The process of e commerce risk management may be exhibited as the figure 2.

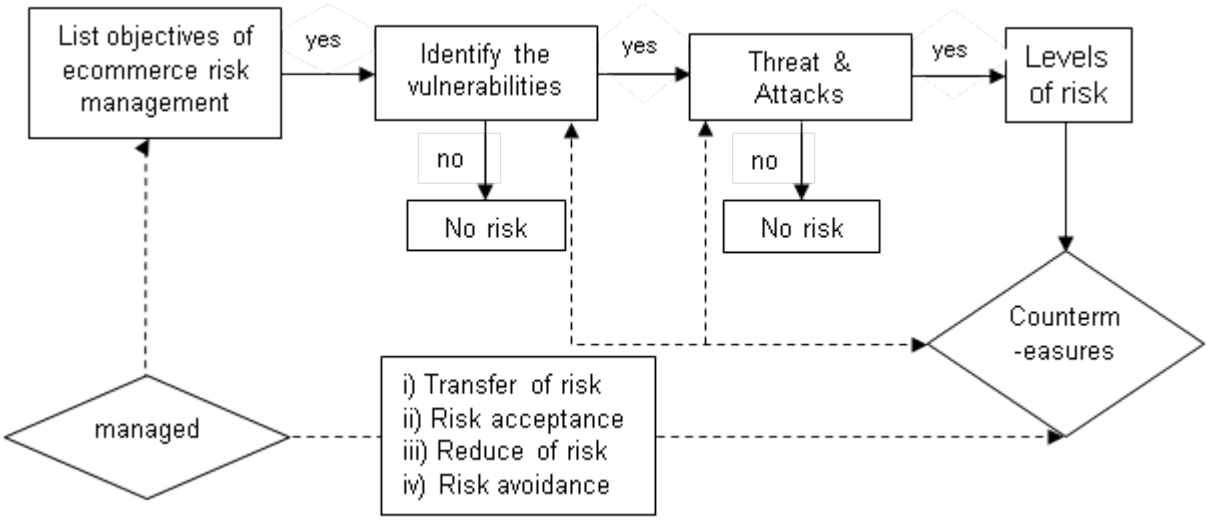

Figure 2. The process of eCommerce risk management

First process of eCommerce risk management is the setting enterprise goals of risk. Establishing the objectives and objects to be protected encompasses all information security requirements. In general, e-commerce risk management needs to ensure all information security requirements. But in practice, in typical situations and conditions, setting of risk management objectives only lead to some information security requirements. For example, the purpose of protecting the customer privacy information stored in e-commerce systems is prioritized rather than maintaining the system in a normal, continuous, uninterrupted manner.

The second process of eCommerce risk management is the analyzing threats and exploiting vulnerabilities. Analyzing threats and attacks on e-commerce systems include also the analyzing vulnerabilities. A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. In eCommerce system, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. The result of the analysis is to detect the types of vulnerabilities, and to answer other questions such as how to exploit the vulnerability, whether easy or difficult, what kind of criminals are likely to detect the vulnerability, How does harm happen? Who suffered? Which targets were violated? ...

The next process is the assessing and ranking risk levels. Because the objectives and objects of risk management are varied, the time of detection of vulnerabilities, types of vulnerabilities and sources of attack, the risk assessment is very difficult. Some risky losses can be quantified. Many cases can only estimate losses, and there are no numerical data. Consequently, there is

subjectivity in rating and risk assessment. However, it is still necessary to make a judgment on the level of risk for specific information incidents.

The last process is the selecting countermeasures. Countermeasures are one or a combination of actions with the use of devices, processes, procedures, or techniques to detect vulnerabilities, mitigate threats, and patch a hole. Countermeasures may also be insured, to prevent an on-going attack by eliminating, or mitigating the damage, loss, or carrying out repairs and restoration of the operating system.

In figure 2, the eCommerce risk manager needs to identify the enterprise's objectives in managing eCommerce risks. The manager needs to identify the eCommerce security requirements. The manager should know which vulnerabilities existing in their eCommerce system. Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets [19]. Thus, threats may exist, but if there are no vulnerabilities, then there is no risk. There is a vulnerability, but if it has not a threat, then there is not a risk.

Suppose they are not detecting any vulnerabilities then they are thinking no risk at all. In contrast, if there is exiting a security vulnerability and the enterprise has used the effective countermeasures, the enterprise may meet no information risk. The manager also has to know which attacks threat to their eCommerce system' s vulnerabilities. There may be no risk if there is no chance of attack. However, there may be some risks that caused from the attacking the vulnerabilities. The eCommerce risk manager needs to assess and rank level of risks. The eCommerce risk manager should know which risk assessment model should be applied? The manager has to decide which countermeasures should be used in business. There are four popular strategies of risk management for applying.

i) Transfer of risk is a measure of risk control used in risk management to describe the shift of the risk burden to another party, for example, sharing loss and damage.

ii) Risk acceptance is a technique of responding to risk. Normally, risk acceptance is adopted as a response to risk when the cost of avoiding the risk is much higher than the cost of accepting it.

iii) Reduction of risk is the using appropriate techniques to reduce the likelihood of an incident, loss or both. For example of risk reduction, a company would be accepting that a disk drive may fail and avoiding a long period of failure by having backups.

iv) Risk avoidance is the using a different" route in which this alternative route may have no risk, lower risk, or lower risk-taking costs. It is the action that avoids any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation options.

Risk assessment model

There are many of risk assessment models. In this paper, we use DREAD model provided by Microsoft. It is part of a system for risk-assessing computer security threats previously used at Microsoft [3] in 2008 and currently used by many corporations. It provides a mnemonic for risk rating security threats using five categories (see Table 2). Each category is given a rating, for example, 3 for

high, 2 for medium, 1 for low and 0 for none. Rating scales run from 0 to 10 are common. The calculation always produces a number between 0 and 10; the higher the number, the more serious the risk, where 0 indicates no impact and 10 is the worst possible outcome [20]. The sum of all ratings for a given exploit can be used to prioritize among different exploits.

Table 2. The DREAD categories

Elements	***Description***	***For example***
Damage (D1)	*How bad would an attack be? If a threat exploit occurs, how much damage will be caused?*	*0 = Nothing* *3 = Individual user data is compromised, affected or availability denied* *5 = All individual tenant data is compromised, affected or availability denied* *7 = All tenant data is compromised, affected or availability denied* *7 = Availability of a specific cloud controller components/service is denied* *8 = Availability of all cloud controller components is denied* *9 = Underlying cloud management and infrastructure data is compromised or affected* *10 = Complete system or data destruction, failure or compromise*
Reproducibility	*How easy is it to reproduce the attack?*	*0 = Very hard or impossible, even for administrators. The vulnerability is unstable and statistically unlikely to be reliably exploited* *5 = One or two steps required, may need to be an authorized user.* *10 = Unauthenticated users can trivially and reliably exploit using only a web browser*
Exploitability	*How much work is it to launch the attack? What is needed to exploit this threat?*	*0 = Advanced programming and networking knowledge, with custom or advanced attack tools.* *1 = Even with direct knowledge of the vulnerability we do not see a viable path for exploitation* *2 = Advanced techniques required, custom tooling. Only exploitable by authenticated users* *5 = Exploit is available/understood, usable with only moderate skill by authenticated users* *7 = Exploit is available/understood, usable by non-authenticated users* *10 = Trivial - just a web browser*

Affected users	*How many people will be impacted?*	*0 = None* *5 = Some users, but not all* *10 = All users*
Discoverability	*How easy is it to discover the threat?*	*0 = Very hard to impossible; requires source code or administrative access.* *5 = Can figure it out by guessing or by monitoring network traces.* *9 = Details of faults like this are already in the public domain and can be easily discovered using a search engine.* *10 = The information is visible in the web browser address bar or in a form.*

Source: Adapted https://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD [20] https://wiki.openstack.org/wiki/Security/VMT-Metrics [21].

DREAD scores five categories, which are summed together and divided by five, the result is a score from 0-10 where 0 indicates no impact and 10 is the worst possible outcome.

Risk Exposure (RE) = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5 [20].

DREAD consists of five elements and It is divided into two groups: Impact and probability. Impact includes two elements: Damage (D1) and Affected Users (A). Probability includes three elements: Reproducibility (R), Exploitability E, and Discoverability (D2).

Damage needs to be assessed in terms of Confidentiality, Integrity and Availability [20]. Damage has three categories and each has been given it's own value ranking from low to high level include trivial, minor, moderate, high, and critical.

Affected users are who suffer damage. Affected users are classified into five groups, including Admin, Power users, Group, User, and the Public.

Reproducibility refers to how difficult to reproduce? And Is it scriptable? Reproducibility has three values, including: complex means the attack is very difficult to reproduce, even with knowledge of the security hole; moderate means The attack can be reproduced, but only with a timing window and a particular race situation; and simple means the attack can be reproduced every time and does not require a timing window.

Exploitability refers to how difficult to use the vulnerability to effect the attack? Exploitability is described into four levels. Expert means the exploit is unpublished, difficult to execute and requires significant insider knowledge and technical expertise or multiple vulnerabilities must be exploited before any impact can be realized. Journeyman means the exploit is unpublished, difficult to execute and requires significant insider knowledge or technical expertise. Adept means the exploit is known including technical and/or insider information but is difficult to execute and no exploit code is available. Novice means the exploit is well known and automated script has been provided that script-kiddies can run to exploit the vulnerability.

Discoverability refers to how difficult to find? Difficult means the vulnerability is obscure, and it is unlikely that users will work out damage

potential. Moderate means the vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.. Easy means published information explains the attack. The vulnerability is found in commonly used features and is very noticeable.

Method of research

Data collection

Describe the problem

In the afternoon 29 July of 2016, hackers attacked the eCommerce system of Vietnam Airlines, the nation's flag air carrier. Ecommerce systems of VietJet Air and Vietnam Airlines including VASCO at the domestic terminal of Tan Son Nhat International Airport, flight information on computer screens for check-in at the check-in counter of Vietnam Airlines, and radio system at the T1 Passenger Terminal of Noi Bai Airport were attacked network intrusion. They must stop operation. Both Da Nang and Phu Quoc airports are in similar condition [8].

Hackers posted derogatory messages with Chinese words distorting the East Sea situation on the flight information screens at Noi Bai and Tan Son Nhat airports, against Vietnam [15]. The VNA website page was replaced by the same picture that appeared on the airports' screens. The access was directed to another web site.

Approximately 90Mb of data has been distributed over the Internet, including more than 400 thousand the airlines' customer database was stolen and made public on the internet.

At the airports of Phu Quoc, Da Nang, Noi Bai, Tan Son Nhat, passengers and ground staff must check in manually. Noi Bai airport has 30 flights, and Tan Son Nhat more than 60 flights delayed from 15 till more than an hour, affect about 2.000 passengers [14, 18].

The way VNA solves the problem [13, 14, 15, 16, 17, 18]

Shortly after the incident, the ground service department has deployed the following activities:

Turn off the monitor and speaker system to inform the customer about the flight,

Staff and passengers checked in the flight in manually,

Using the portable speaker to announce the flight to the passenger,

Report to authorities and call for support to handle the accident. Several authorities in Ministry of public security of Vietnam have been mobilized to handle the incident, such as A85, A68.

After 15 hours, the problem has been resolved. Vietnam Airlines 's check - in system has been repaired and returned to normal.

In addition, VNA advised its members to change their account passwords as soon as the network system is recovered

Some opinions of experts of VNA's incident [16, 18]

This attack may have been prepared for quite some time. This is a sophisticated attack. Attackers used malicious code that not detected by antivirus software. Attackers have broken into important systems and controlled the VNA' portal and customer database. Many computers and electronic means in various parts of the VNA are also infected virus. Hackers launched attacks in multiple locations and at the same time. This has increased difficulties for the VNA.

Experts comment on VNA's risk management [16, 18]

VNA has lacked a good plan to protect the e-commerce system, to monitor and detect early signs of abnormalities. Vietnamese security experts have warned VNA' e commerce security vulnerability before the incident, however, VNA has not taken countermeasures timely. As soon as the incident occurs, VNA has taken many measures to minimize the damage.

Analysing VNA incident

Apply the DREAD model to explain the elements in the first column, describe each of the details in the second column, and indicate the reason in the third column, and the final column as the score.

Table 3. Analysing VNA incident used DREAD model

Elements	***Description***	***Rationale***	***Evaluated***
Damage	*Aircraft computer systems, flight information screens, computer monitors for check-in at check-in counters, radio systems to stop working. More than 100 flights delayed. Over 400 thousand the airlines' customer database was stolen and made public on the internet*	*Infringement on availability requirement. Confidentiality of information is compromised*	*6 to 8 point*
Affected users	*More than 100 flights were affected, of which dozens of flights were delayed by 15 to 60 minutes. Staff and passengers checked in the flight in manually, using the portable speaker to announce the flight to the passengers*	*Admin, power users, group, user, and public. All five groups were affected*	*7 to 8 point*
Reproducibility	*The website of Vietnam Airlines has been re-activated, but according to security experts have not yet patched the vulnerabilities and the risk of recurrence*	*Moderate or simple*	*4 to 5*
Exploitability	*This is a sophisticated attack. Attackers used malicious code that not detected by antivirus software.*	*Expert Or Journeyman*	*8 to 9 point*
Discoverability	*According to Vietnam security experts, the vulnerability on the VNA eCommerce website have warned long before the incident*	*Easy or moderate*	*3 to 4 point*
Range of Risk Exposure score = 5.6 to 6.8 point means ***Important***			

Discussion

DREAD score ranges from 5.6 to 6.8 indicates that VNA incident is not a particularly serious problem. If DREAD's score is over 7 point, It is critical [4, 20]. From analysed results, we see in five elements D1, R, E, A, D2, only E element explains the Attackers are Expert or Journeyman. Two R and D2 elements explain the reproducibility is simple or moderate only, and discoverability is easy or moderate. Damages are large and many users are affected.

I also agree with expert' opinions on risk management in the VNA. Risk management is the process where the identification of risk management objectives, the assessment of threats, losses occurring as well as the selection of risk countermeasures must be carried out in a uniform manner. Any part of the process that is underprivileged leads to unpredictable consequences. Data analysis shows that VNA has been warned about the vulnerabilities, but VNA has not taken appropriate countermeasures timely. VNA does not foresee the possibility of loss is very serious. Although VNA identified the possibility of attack two days ago, and actively isolate the flight control system (this system is not connected to the Internet so not attacked), but it takes up to 4 minutes to turn off the screen and audio system indicating that VNA has not responded to the problem in the fast. Naturally, this is an information risk because if VNA knows certainly the attack, then VNA will apply a suitable response, there is no chance for the incident. Even if the vulnerability has been patched, it may still be vulnerable to the attack where it has been patched, so the VNA site administrator may ignore this warning. On the other hand, the attack has been very well prepared, so the VNA's encountermeasures can be accepted.

Conclusion and recommendation

This paper has provided an empirical research on eCommerce risk management through the using DREAD model for analysing the VNA incidents. Learning lessons from VNA experience, other e-commerce enterprises in Vietnam need to understand the process of information risk management and strictly implement the process. Enterprises must be proactive in preventing and combating attacks to minimize any damage. Even if an attack is inevitable, they must also use suitable measures to minimize the damage.

References:

1. Alessandro Deidda (2009), A New Standard for Security Risk Management, ISO/IEC 27005:2008, Symantec
2. Anni Piiparinen (2016), China's Secret Weapon in the South China Sea: Cyber Attacks, http://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/
3. Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002), Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30
4. Hengzhe Li (2011), Threat Modeling, Microsoft Security Development Lifecycle (SDL)

5. Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46
6. ISO / IEC 27000: 2009, Information security management systems — Overview and vocabulary, https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-1:v1:en
7. ITU (2015), Global Cybersecurity Index & Cyberwellness Profiles
8. Martin Petty (2016), Hackers hit Vietnam airports with South China Sea messages, https://www.reuters.com/article/us-vietnam-hacking-idUSKCN1091YL
9. Pooja Kungwani (2014), Risk Management- An Analytical Study, Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 16, Issue 3. Ver. III (Feb. 2014), PP 83-89
10. Vietnam national assembly, Information Security Act 2015
11. William Stallings (2014), Cryptography and Network Security: Principles and Practice, Sixth Edition, Pearson
12. Wu Yanyan (2014), Research on e-commerce Security based on Risk Management Perspective, International Journal of Security and Its Applications Vol.8, No.3 (2014), pp. 153-162.
13. Chinese hackers attack VN's airports and Vietnam Airlines' website http://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html#ADrOeQGUzEm0qtDP.99
14. Vietnamese airports hackings, https://en.wikipedia.org/wiki/Vietnamese_airports_hackings
15. Hackers target flight info screens at Vietnam's airports, http://www.dw.com/en/hackers-target-flight-info-screens-at-vietnams-airports/a-19437977
16. Cyber-terrorists attack flight info screens at Vietnam's 2 major airports http://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html
17. Hackers hit Vietnam airports with South China Sea messages https://www.reuters.com/article/us-vietnam-hacking-idUSKCN1091YL
18. Malware attacking Vietnam Airlines appears in many other agencies, http://security.bkav.com/home/-/blogs/malware-attacking-vietnam-airlines-appears-in-many-other-agenci-1/normal?p_p_auth=DHFn7deT
19. http://acriafrica.com/risks.htm African Cyber risk Institute
20. https://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD
21. https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD