The vulnerability of cyber security and strategy to conquer the potential threats on business applications

Muhammad Altaf Mukati and Syed Muzammil Ali
SZABIST Karachi, Pakistan
altaf.mukati@szabist.edu.pk and Smuzammilali@gmail.com

***Abstract*—Web technology has become an important part of online business such as sharing information, social interaction, activities related to business especially online payment methods, credit card information, bank transactions, online banking and many other applications. The exponential use of web technology introduces new possibilities of criminal activities and creates unbearable threats to the information and business trades. This is mainly because of the widely use of the World Wide Web and cloud computing for information sharing and saving regardless of the user.**

As technology grows with the passage of time, the web technology becomes more advanced and complex in terms of security and privacy and drives new challenges and threats which makes the internet unsafe for business applications. Many of the currently available applications have loopholes which makes cyber criminals to exploit the applications easily. The main vulnerabilities are Cyber theft, vandalism, web jacking, credit card information stolen, privacy and security issues, cyber terrorism, spam and etc. An ongoing challenge related to cyber security community is related to handle the transition of technology to commercial or open source web applications available in the market. This paper provides the strategy to overcome the vulnerabilities and potential threats to the business applications.

Keywords: Cyber security; Web security; Vulnerabilities; Web based small business applications; Security threats; XSS; Validation

I. Introduction

The history shows that criminal activity in the cyber world has produced great losses to the financial sector or individuals and has shown and upward trend in the recent times, even the governments and intelligent services undergoing numerous amounts of losses in terms of valuable information in the cyber world.

The crime environment is totally different in the cyber world which is causing difficulties enforcing crime laws in the real world. To understand the nature of the cybercrime, let's consider an example of the age factor which is self-authenticating parameters so children's under age of 18 can easily break the rule and access the restricted content where in the real world he can easily be detected and enforced while computer technology is dependent on the user itself to identify his/her age [1].

Cyber security provides the shield against all the crimes and unauthentic access of the restricted information and protects the data by deterrence, discovering and answering to the potential threats and attacks. The cyber security is not just dealing with the networks and computer but also includes the traditional crimes involves internet activity such as hatred crimes, negative marketing, frauds, identity theft, credit card information stolen using mobile and internet.

According to the head of new cyber command in USA:

"Pentagon's systems are probed by unauthorized users about 6 million times a day. Total losses are, through cybercrime globally, may be as high as 1 trillion dollars" [3].

II. Cyber Security

Internet is an essential tool required in our daily lives for instant anything you want is a click away such as: online shopping, banking, payrolls and etc. However being exposed to Internet might require few safety measure so other people such as cyber criminals, who could steal valuable information through the internet without anyone having a clue about it. If you want own a small or medium business, you might to protect your valuable information from getting into the wrong hands. You could do that through following few steps such as: Office computers should only be utilized for strictly business purposes

Cyber security is about how one can protect themselves against cyber criminals. It is supported by three essentials goals such as:

1. Confidentiality: No one but authorized personnel should be granted access to important files.
2. Integrity: A person reliable enough should be held in charge so there are is no chance of the information to get leaked.
3. Availability: The information should be available when either asked by the business itself or its clients.

A. Cyber Theft

In cyberspace, Cyber Theft is the most common cyber-attack committed. In the generic terms Cyber Theft is known as hacking. Its process is very simple just with the help of computer they can steal information or assets. They usually use tactics such as, piracy, hacking, embezzlement, espionage, plagiarism, DNS cache poisoning, and identity theft. Moreover, it can also give the illegal access of the system without the user's knowledge or consent, also for stealing/tampering the precious confidential data and information. It can be done by using the malicious script to break/crack the computer system. Usually IT companies like;

Microsoft, Yahoo, Amazon and other financial firms are victim of such attacks. Cyber Theft is among the gravest cybercrimes nowadays.

B. Cyber Vandalism

Cyber Vandalism is retained to corrupting or damaging the data unlike Cyber Theft for stealing or misusing it, Vandalism destroys the data however; it can also be used to disrupt or stop the network services. This can also deny the access to the information contained on the network to the authorized users; such as; employees or website visitor. This cybercrime can be dangerous as time bomb, the programmer can set a virus to be activated itself at a specified time to damage the targeted system. The most scary part is without the permission of the owner of the network this can cause irreparable damage to the systems, deliberately entering malicious code or viruses into a computer networks to monitor, follow, disrupt, stop or perform any other action. This is why they are severe kind of cybercrimes.

C. Web Jacking

Web jacking can be a powerful control of a web server from which it can gain the access and control affected website over the web. It can also be used to manipulate the information on the sites by hackers. For example in the case of "Gold Fish" the hackers hacked the site and changed the information pertaining gold fish. Further a ransom of US dollar 1 million was demanded a ransom.

D. Stealing Credit Card information

Stolen the credit card information from the ecommerce websites using different techniques of hacking and breaking the server and misused the credit card information for other purposes.

E. Software Piracy

Distribution of the illegal copy of the software without the knowledge of the owner by distributing it public forms such as peer to peer free sharing software, broadcasting freely and unauthorized download of the application.

F. Industrial Espionage

Spying of the competitors company by monitoring there network traffic and using some other tactics to stolen there business, marketing, products and even financial information.

G. Cyber Terrorism

Using the computer technology to increase society violence against civilians mostly because of the political affiliations and other illegal activities using social networking or other internet technology.

H. Cyber Contraband

Transferring illegal information using internet which is banned because of the location constraint or some other reasons. Such as using anonymous proxy websites to gain access of the illegal or banned websites from internet.

I. Spam

Unauthorized content send to the participant email addresses by violating the laws of spam such as illegal marketing and immoral content, commercial applications and other banned products.

J. Wi-Fi High Jackin.

Illegal access of the unsecure devices connected to some private wireless networks. Studies shows that most of the private networks are widely open in the cyber world which gives opportunities for hackers to provoke the situation and exploit the unsecure devices

K. Cyber Trespass

To get the access of the victim's private information without his/her knowledge by spying the devices or networks without damaging or disturbing the data. By snooping the networks or other resources to gain access of the important information without damaging or distributing it.

L. Logic Bombs

Malicious script or programs dependant on some events and activated only when some event occur such as on any particular date, when accessing any particular file or resource. This can exploit network or devices only when some events occur.

M. Drive by Download (Gumbler)

The term "Drive by Download (DbD)" is maneuvering in software industry since its inception with different variations. In this case it attacks the users while they are surfing on the internet the software is automatically installed on the user's computer. However, the reason behind installing these software's onto the computer is to gain benefit over victim server, such as, stealing important information, which could be personal data, passwords or using victim terminal as bonnet to further spread malicious contents. A recent survey done by Google Inc. shows that, as many as 1 in 10 websites were acting as hosts for malware.

N. Salami Attack

Salami attacks are usually known for financial crimes. How it works is, they launch software to modify the transaction, just a small amounts such as cents or pennies are deducted from the transaction and redirect them into a hidden account. For example a logic bomb can be installed in the bank's system, which will only deduct 1/2 cents from every account and deposited it in a particular account. The worst thing about this type of crime is, they take so small slices from the transactions that nobody even notices, so it becomes very hard to get caught.

O. Cyber Assault by Treats

With the usage of computer, internet or network device such as mobile phone, call recording, video or email address threatening a person to the fear of his relationship, assets and their lives. An example of such case would be like to threaten a person to much extent that he transfers the money to untraceable bank account.

P. Script Kiddies

These scripts develop by some professional hackers to attack on victim's computers, devices or networks to get the root access or administrative access to exploit the information. These are pre-written malicious scripts available in the black market.

Q. Deniel of Service

This is an attempt to busy the victims computer, device or network to be unavailable when needed such attacks are called denial of service attack (DoS) and also known as distributed denial of service attack (DDoS). In this attack the victims' computer are overloaded with the process than it can handle which results as crash of the device.

To tackle the cyber theft different companies don't have any policy and they just try to install any antivirus and spyware to protect the information which is not the right way to protect the data. It's very important to understand the nature of the problem before providing any solutions [7].

III. Cyber security strategy

With growing number of cyber-attacks on various industries tends to reach an unacceptable security risk which needs to be handle in-order to protect the industry from great losses. Yet, even some executives with cyber awareness are not willing to seriously take actions and acknowledge the issue.

The strategy to protect the businesses needs to be designed and engineered systemically by using the latest technology and brightness minds so defense go beyond firewalls and are able to defend the threatening cyber-attacks. Some of the techniques can easily enhance the cyber security against potential threats are as follows:

A. Risk Assessment

The very first step towards the cyber security against the potential threats is to assess the risks involves like networks or system failures. The API standard 1164 also recommend to take first step towards cyber security is to evaluate the risks facing the industry or business. The system should be design with the most effective contingency planning and priorities the counter measures. Risk management should be administrated to provide the necessary recommendations and documentations for the plan assessment.

B. Protection

In general most of the business industry has some kind of protection against cyber-attacks. However, most of them consider firewalls, antivirus, anti-spyware and access control systems to protect from unwanted vulnerabilities to their businesses. But most of them are dependent on updates if it's outdated then it can be easily bypass by the potential attacker. If the system is encountered with the latest cyber-attack and system firewall and protection shield is not aware of it then it provide no defense against this threat. It can be enhanced by providing only the authorize members to access the critical areas while considering the alternative approaches towards the protection of the system.

C. Monitoring

The approach is a constant monitoring of the system and activities on the process control network. Firewall and other protection techniques can easily bypass so it's the important part to monitor the systems regularly for any new potential cyber-attacks. The nature of the monitoring can be programmatic but should not be periodic it should be ongoing and consistent.

D. Detection/Reaction

The most critical part to outline the cyber security threat is to have proper detection/reaction strategy. Once the threat is detected by monitoring the response plan is activated. If we consider an example of one attack called DOS denial of service can cause the web inaccessible so if we have a plan to recover the web services as soon as monitoring system detect the attack we can easily over the risk of any attacks.

E. Outthink the hackers

Proactive plans are always vital and can save the industry from great losses; the time of ignoring "the elephant in the room" has passed. Pre planed the risk management and take necessary actions towards cyber-attacks can save the industry from cyber-attacks to some great extent.

It's a continuous lifecycle to insure the cyber security to some extent. The fig 6 describes the steps involved in the cyber security to priorities assets, risks monitoring, responding and taking necessary actions when it requires safeguarding the system.

Recent reports shows that most of the applications available online have vulnerabilities; these are the most common issues of current web security and their countermeasures.

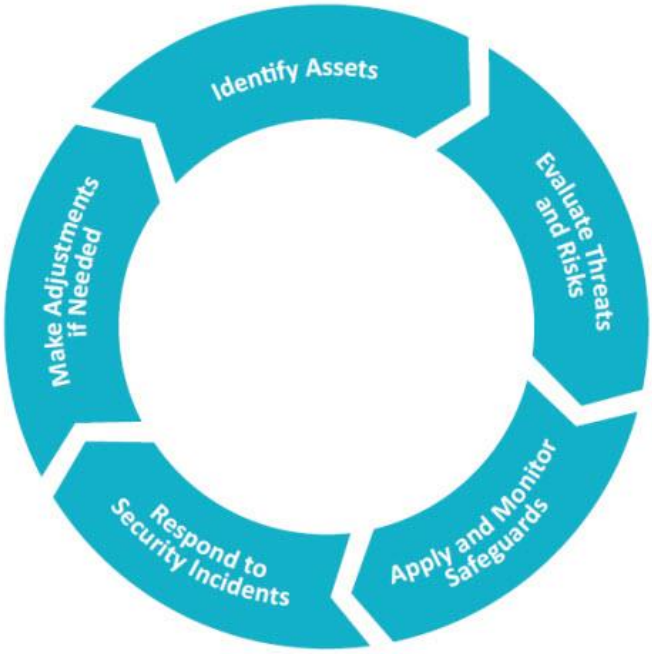

Fig. 1. Cyber security fundamentals [10]

IV. Cyber security solutions

A. *Invalidated input (The most common security threats)*

In this attack the hacker can easily tamper the any part of the HTTP request on client side even before submitting the form or a web page.

- URL
- Cookies
- Sessions
- Forms (Input and hidden fields)
- Headers

The most common names used to refer tampering attacks are as follows

- Forced browsing
- Command insertion
- Cross site scripting
- Buffer overflows
- Format string attacks
- SQL injection
- Cookies poising
- And hidden fields manipulation

The solution for these kinds of common issues is to validate the data before submitting to the server including all parameters on both client side and server side. The problem with the client side validation is that it can be easily manipulated by the attackers but it's mainly because to get the quick response for the users for common validating issues. It's also import to do canonicalization of input data which is referring to simplify the process of encoding and decoding.

Used the centralize way of coding for input validation, scattered code create more problems to manage the input validation. Each parameter should be validated according to the specified input which is allowed to submit, this term also known as positive validation. The negative approach which is relying on the filtering out some disallowed inputs and is difficult to manage such approaches.

Validation Criteria

- Data type (string, integer, real, etc…)
- Allowed character set
- Minimum and maximum length
- Whether null is allowed
- Whether the parameter is required or not
- Whether duplicates are allowed
- Numeric range
- Specific legal values (enumeration)
- Specific patterns (regular expressions)

```
public void doPost(HttpServletRequest req,…) {
  String customerId =
    req.getParameter("customerId");
  String sku = req.getParameter("sku");
  String stringPrice = req.getParameter("price");
  Integer price = Integer.valueOf(stringPrice);
  // Store in the database without input validation
  // What happens if a hacker provides his own
  // price as a value of "price" form field?
  orderManager.submitOrder(sku,customerId,price);
} // end doPost
```

Fig. 2. Example code to illustrate the validation problem

```
public void doPost(HttpServletRequest req,…) {
  // Get customer data
  String customerId =
    req.getParameter("customerId");
  String sku = req.getParameter("sku");
  // Get price from database
  Integer price = skuManager.getPrice(sku);
  // Store in the database
  orderManager.submitOrder(sku,customerId,price);
} // end doPost
```

Fig. 3. Example code to illustrate the solution for the input validation problem

B. *Broken access control*

The security policy is one of the important requirements for the web applications access control system. It's highly recommended to use the access control matrix to implement the access control rule. Access control testing requires extensive testing to prevent the possible attacks and need variety of account to test and may attempts to access unauthorized control or functions. These are the following terms refer to the broken access control

- Insecure ID's
- Forced browsing pass access control checking
- Path traversal
- File permissions

Most of the web application using the default index structure like ids, user reference key and etc. if attacker can guess the index key then it's easy to comprise the other user information.

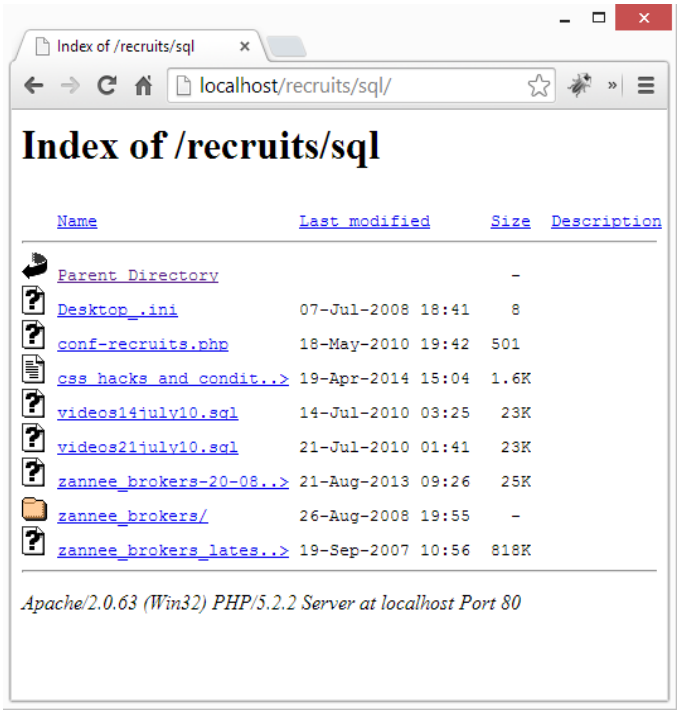

Fig. 4. Exposing the directory structure of the database files

C. *Broken authentication & session management*

Include all features of handling user authentication and management of the active sessions. Session hi-jacking where session are not really protected and can easily be compromised user identity.

```
public void doGet(HttpServletRequest req,…) {
  // Get user name
  String userId = req.getRemoteUser();
  // Generate cookie with no encryption
  Cookie ssoCookie =
            new Cookie("userid",userId);
  ssoCookie.setPath("/");
  ssoCookie.setDomain("cisco.com");
  response.addCookie(ssoCookie);
  …
```

Fig 5: Broken Account/Session Management (Client Example—SSO)

```
public void doGet(HttpServletRequest req,…) {
  // Get user name
  Cookie[] cookies = req.Cookies();
  for (i=0; i < cookies.length; i++) {
    Cookie cookie = cookies[i];
    if (cookie.getName().equals("ssoCookie")) {
        String userId = cookie.getValue();
        HttpSession session = req.getSession();
        session.setAttribute("userId",userId);
    } // end if
  } // end for
} // end doGet
```

Fig. 5. Broken account/session management (Server Example—SSO)

```
public void doGet(HttpServletRequest req,…) {
  // Get user name
  String userId = req.getRemoteUser();
  // Encrypt the User ID before passing it
  // to the client as part of a cookie.
  encryptedUserId = Encrypter.encrypt(userId);
  Cookie ssoCookie =
    new Cookie("userid",encrypteduserId);
  ssoCookie.setPath("/");
  ssoCookie.setDomain("cisco.com");
  response.addCookie(ssoCookie);
```

Fig. 6. Safe account/session management (Client Solution—SSO)

```
public void doGet(HttpServletRequest req,…) {
  // Get user name
  Cookie[] cookies = req.Cookies();
  for (i=0; i < cookies.length; i++) {
    Cookie cookie = cookies[i];
    if (cookie.getName().equals("ssoCookie")) {
          String encryptedUserId = cookie.getValue();
          String userId = Encrypter.decrypt(encryptedUserId);
          if (isValid(userId)) {
                HttpSession session = req.getSession();
                session.setAttribute("userId",userId);
          } // end if isValid…
    } // end if cookie = ssoCookie…
  } // end for
} // end doGet
```

Fig. 7. Safe account/session management (Server Solution—SSO)

D. *Cross site scripting counter measures*

One of the most common methods is to validate inputs including all the system variables which are especially used in OS as a parameter, scripts and database queries to prevent the possible cross site scripting (XSS). Encoding of the users supplied code is important in-order to prevent the executable scripts from users end. To protect the code from JavaScript attacks by encoding these special characters as follows:

- From "<" to "<"
- From ">" to ">"
- From "(" to "("
- From ")" to ")"
- From "#" to "#"

- From "&" to "&"

```
protected void doPost(HttpServletRequest req, HttpServletResponse res)
   {
   String title = req.getParameter("TITLE");
   String message = req.getParameter("MESSAGE");
  try {
     connection = DatabaseUtilities.makeConnection(s);
     PreparedStatement statement =
       connection.prepareStatement("INSERT INTO messages VALUES(?,?)");
     // The "title" and "message" are saved into
     // the database.  These "title" and "message"
     // might contain ill-intended JavaScript.
     statement.setString(1,title);
     statement.setString(2,message);
     statement.executeUpdate();
   } catch (Exception e) {
     …
   } // end catch
} // end doPost
```

Fig. 8. Cross-scripting problem in the script

```
private static String stripEvilChars(String evilInput) {
   Pattern evilChars = Pattern.compile("[^a-zA-Z0-9]");
   return evilChars.matcher(evilInput).replaceAll("");
}
protected void doPost(HttpServletRequest req, HttpServletResponse res) {
  // Do vigorous input validation
  String title = stripEvilChars(req.getParameter("TITLE"));
  String message = stripEvilChars(req.getParameter("MESSAGE"));
  try {
     connection = DatabaseUtilities.makeConnection(s);
     PreparedStatement statement =
       connection.prepareStatement
         ("INSERT INTO messages VALUES(?,?)");
     statement.setString(1,title);
     statement.setString(2,message);
     statement.executeUpdate();
   } catch (Exception e) {
     …
   } // end catch
} // end doPost
```

Fig. 9. Cross-scripting solution

E. Improper error handling

In the development process ensure that the all web application related errors are handled maturely. So when ever error occurs application should handle properly send notification and display specially design results which is helpful to the users and hide unnecessary information. Error logs should be maintained to properly diagnose the nature of the errors and fix them accordingly.

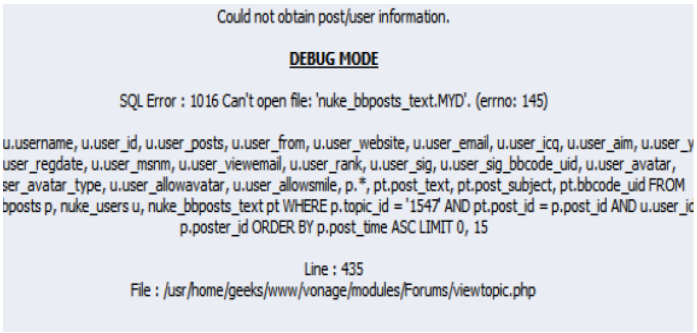

Fig. 10. Some error showing all the structure of the SQL table

V. PROPOSED SOLUTION

I have developed simple easy to implement script which can be installed on any web application easily. The main purpose of the application is to provide the easiest way to identify the most common vulnerabilities of the web security. Once we identify the possible attacks on the application then we can take necessary actions accordingly in-order to save time and resources on unnecessary security measures for small limited budget web applications. Once we identify the potential threatening loophole in the application we can take necessary countermeasures. Because most applications on the web has cyber security vulnerabilities but actual problem is the acknowledgement of the issue. My script has the capability to identify the common web security vulnerabilities and notify the end users about the possible attacks.

I have implemented my script on some of the online applications and amazed to see the results, I am getting daily three to four notifications about the possible attacks.

It is simple to implement and any user can get notification on any email about the webpage vulnerabilities. The sample script can be shown in the fig 19.

```
<!--
    // Embed code should be copied under the header of the web page
    // to monitor possible cyber security attacks
-->
<script type="text/JavaScript">
var clientEmail = "sample@email.com";
</script>
<script type="text/JavaScript" src="http://www.zannee.com/research/script.js"></script>
```

Fig. 11. Sample script to embed on any page to get the notification of the possible attacks

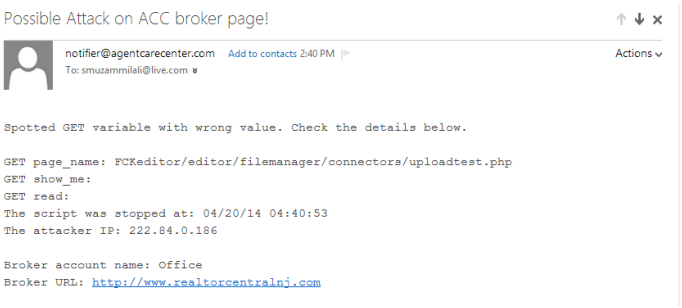

Fig. 12. Showing the sample notification email for the possible attack.

CONCLUSION

In the current era of the web applications every business is going online for its survival and the use of the small business applications increase to some good extent and share all related resources and information on the web server for online availability. To make these resources safe and secure each organization needs to follow some rules, regulations and guideline to implement cyber security policy. But most of the solutions are static in nature and required time and resource to implement such policies which is difficult for the small business organizations to handle the cyber security threats with limited budget and constraints. Hence there is a need of dynamic solutions and also an easy solution that can serve the purpose and provide basic guideline toward securing the web application with the most common security threats. Proposed solution provides the information regarding the possible attacks on the web application, so that small business owners can take quick actions to prevent greater lost.

FUTURE WORK

There is a need of a semantic solution that can predict/understand the nature of the context that leads to the potential cyber vulnerabilities.

ACKNOWLEDGMENT

Many thanks to Dr. Muhammad Altaf Mukati for supervising this study and providing his technical knowledge and support in all matters.

REFERENCES

[1] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," *2013 IEEE Elev. Int. Symp. Auton. Decentralized Syst.*, pp. 1–6, Mar. 2013.

[2] Maughan, D., Balenson, D., Lindqvist, U., Tudor, Z. "Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice" *Security & Privacy, IEEE (Volume:11 , Issue: 2)*, pp. 14–23, April 2013.

[3] Dupont A. "Time to attack cybercrime with a strong security policy" http://www.smh.com.au/federal-politics/political-opinion/time-to-attack-cyber-crime-with-a-strong-security-policy-20101012-16ho5.html, October 2010.

[4] Kshetri, N, "The global cybercrime industry: economic, institutional and strategic perspectives" , Springer, 2010.

[5] Collier, Z., Vicksburg, DiMase D., Walters S., Tehranipoor, M. "Risk-Based Cybersecurity Standards: Policy Challenges and Opportunities". In Computer (Volume:PP , Issue: 99). Jan 2014

[6] R. Kozik and M. Chora, "Current Cyber Security Threats and Challenges in Critical Infrastructures Protection," pp. 93–97, 2013.

[7] N. K. Sangani, P. Velmurugan, T. Vithani, and M. Madiajagan, "Security & Privacy Architecture as a service for Small and Medium Enterprises," 2012 Int. Conf. Cloud Comput. Technol. Appl. Manag., pp. 16–21, Dec. 2012.

[8] Douglas Maughan, David Balenson, Ulf Lindqvist, and Zachary Tudor, "Crossing the 'Valley of Death '" *SRI International*, 1540-7993, April 2013.

[5] WhiteHat Security, "Website Security and Statistics Report", http://www.whitehatsec.com/resource/stats.html , May, 2013.

[6] G. G. For and M. Businesses, "Know the Risks. Protect Yourself. Protect Your Business.", http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-eng.aspx, 2013