Managing Risks of Managed Webhosting Outsourcing

Kalpin Erlangga Silaen\textsuperscript{a}, Dr. Mohammad A. Amin Soetomo\textsuperscript{b}

\textsuperscript{a}Swiss German University, EduTown BSDCity, Tangerang 16339, Indonesia
\textsuperscript{b}Swiss German University, EduTown BSDCity, Tangerang 16339, Indonesia

ABSTRACT

Outsourcing managed webhosting to the provider can give benefits from cost savings point of view. With outsourcing webhosting, company can focus with their core business without worrying how to manage their webhosting, backup, hardware, software and licenses. Unfortunately, this also raised security issues and impact business. This paper provides another insight about risks in webhosting outsourcing and a model to manage those risks based on NIST SP800-30.

Keyword: Managed Webhosting; Outsourcing; Risks Management

1. INTRODUCTION

Outsourcing webhosting is purchasing webhosting services from other provider where consumer can put their contents to provider's server to serve their visitor or clients. This is called outsource because in fact, internally, the consumer can provide this kind services [1], but for one or more reasons, company decide to use other provider to host their website. NIST SP800-145 defines webhosting as Software as a Service (SaaS) where consumer can use provider's application to run their website and display to visitor. However, the consumer does not have control to hardware, operating system, server's configuration, and network [2]. The consumer can use storage, power of server and bandwidth as much as their subscribe to the provider. Furthermore, managed webhosting means the consumer can ask provider's assistance to help and fix any issues related to their services in webhosting. Scope of managed webhosting depends of agreement between provider and consumer. For example, the provider may provide basic managed webhosting for optimizing performance of consumer's website, or provide gold managed webhosting which include managing backup, monitoring performance, and other services. Basically, webhosting provider without managed services only provide space or capacity, power of computing, control panel to manage webhosting, and basic access such as FTP access to the server where consumer's website allocated. Based on the way managing resources, webhosting service usually has two models, shared hosting and dedicated hosting [3] with managed services as add-ons for both models. This paper discuss about managing risk in webhosting outsourcing based on NIST SP800-30 and how an organization or business consider to use webhosting outsourcing.

2. RELATED WORK

Some researchers have been discuss about risk in webhosting and related to cloud hosting with different approach. Currie. L. Wendy [4] discuss about outsourcing of web application, where consumer can use it with model pay-as-you-go, but the research does not discuss about security in webhosting environment. Charles Kubicek [5] studied about QoS (Quality of Service) for webhosting environment. His research focus about performance of webhosting based on response time. Performance is one of important point for webhosting services, but this paper will focus about risks and how to manage it. Ioan Petri et all [6] discussing about risk assessment in service provider and propose SLA (Service Level Agreement) and trust mechanism as risk mitigation for services. In delivering SLA, provider provide server farm to reduce unavailability, but they studied from provider's point of view. In this paper, we are discussing about risk in using outsource webhosting with literature review methodology.

3. FLOW PURCHASING WEBHOSTING
Usually, consumer decide to purchase webhosting from advertising of provider in other websites, and search from search engine without deep analyze about provider. Later, consumer also search about review from other people about provider. For example, if a consumer has 3 candidate of webhosting provider, they can search about review good or bad in internet. Unfortunately, this is sometime bias. Some provider can also send their sales or people to write false good review and spread it to internet. For managed hosting, since consumer will have intensive communication, consumer need to know deeply about their potential webhosting provider, so they usually invite them to meet and present their product to consumer. The consumer, if they need a specific needs, they can ask potential provider if they can provide it. In this case, provider needs to bring a product expert, like presales person to discuss about consumer's need and how it works with their product, and consumer can ask detail about their Term of Services (TOS) and Acceptable Use Policy (AUP) because this is related to legal [7]. Also, consumer can ask about provider's SLA [6][7] and compliance if needed. Compliance needed by consumer if regulator enforces them to comply, for example, consumer who runs e-commerce may enforced by local regulator to meet some requirements, even if it is not core's web application (for example, blog website, news website, etc but related to their business). In general, purchasing webhosting service can shown like picture below:

Choosing Webhosting Provider Flow

The figure above shown that consumer and potential provider (term before agreement) need create good communication and understanding. Potential provider must show their honest and consumer also must tell them what they need, what they expect from webhosting provider.

4. BENEFITS OF OUTSOURCING WEBHOSTING

4.1. Cost Savings

Company who decides to in-house their webhosting should provide man power to manage their infrastructure, including servers, rack, space, power of electric, HVAC (Heating, Ventilating, and Air Conditioning) which is need more resources to manage all of them. Also, they have to ready provide
helpdesk, support, system expert for 24 hours a day. This situation can increase operational cost significantly. In other side, company who decides to outsource their webhosting to other party, not only can save big cost, but also they can focus with their core business. Talking about infrastructures such as servers, router, switch, and other device also concerns about TCO (Total Cost of Ownership) [1] which is difficult to manage, especially if company is not IT related business and does not have experience about managing IT project. With outsourcing webhosting, company just pay small amount to provider and they can start put their content to the server and publish it to internet or for their own usage. But company also must aware about what contents they can put to outsourcing webhosting to avoid any risks in case there is security breach or regulation rules. Of course, if there is critical information or valuable information, company does not have reason to pay only $5 a month to host them to outsource webhosting. Those issues will discuss in next risk management.

4.2. Availability

In-house webhosting for some company with good support also has some problem, availability [8]. In security, availability is one of triad CIA (Confidential, Integrity, Availability) [9] which is include in risk assessment. More questions about availability in-house webhosting are:
- Does company provide redundant power?
- Does company provide redundant internet link?
- How fast company can replace any fault hardware?
- Does company environments support for good connectivity, electric, flood, and other threats?

For internal web application, such as internal portal and any internal consumes website, there is no problem for in-house hosted them internally as long as they do not have any branch or partner at other location which need to access them. Usually webhosting company has datacenter or at least they have space in datacenter with good inter-connection with redundant link to internet (for good webhosting provider who cares about their quality link and provide good SLA). Datacenter also provide redundant power electric and provide 24 hours support and with additional managed services, they can also provide on-hands support (for example, replace hardware in covered SLA, monitoring, and other administration support). Some provider can also provide multiple locations based on their promise SLA to their client.

In other words, company has good reasons to use outsource webhosting, saving cost and good availability. But still they need to know about security aspect, any risk may impact to their business and how to mitigate them.

4.3 Scalability

Advanced webhosting technology especially if they are true cloud, provider can provide an interface where consumer can upgrade or downgrade their resources based on their needs. Nowadays, more provider already have this feature, consumer subscribe to basic resources and with click and go, they can resize their subscribed resources without losing their data. This make consumer has ability to reduce cost which is already low.

5. RISK OF OUTSOURCING WEBHOSTING

NIST SP800-30 defines risk is a probability of an event from threat with negative impact to objectives because of existences of vulnerability. Risk management is a process to assess, identify risk and take necessary steps to mitigate them to the acceptable level [8]. Webhosting in general has some types of risks such as hacking (deface, information leakage, etc), data loss, disruptive event [10] (denial of services, distributed denial of services, power fault). Azeem Aleem et. al [7] find that data leakage is in position 1 for top cloud threat, and insider threats in position 3 which maybe involve provider. For outsourcing webhosting, there are some risks such as legal or regulation which may not allow company to outsource their webhosting to other party, or at maybe regulator requires that provider also must provide standard as requirements. In this case, company need to work together to provider to solve this kind issue. In outsourcing webhosting, trust mechanism, transparency, good communication also need to establish between consumer and provider. In shared environment, there is a possibility of abusive resources which impact to performance of other tenants or user, so provider need to implement some technology to manage those resources [11][12].

6. RISK MANAGEMENT
6.1 **RISK ASSESSMENT and ANALYSIS**

Risk assessment is a method to help company define any risk which maybe occurred. The output of risk assessment will become input for risk analysis. Risk analysis provides company about comparisons between cost and benefit for any applied protection to mitigate risks. Risk assessment methodology has nine primary steps [8] with associated between input and output as shown in Figure 2.

![Figure 2. Risk Assessment Methodology in NIST SP800-30](image)

### 6.1.1 System Characterization

In this initial step, company can ask provider any details about their system before they decide if their system is acceptable to their business. Later, company can cross check this information from other trusted sources to see if provider is honest. An example form of system assessment for outsourcing webhosting can see as table 1 below:

<table>
<thead>
<tr>
<th>Assessment Point</th>
<th>Physical</th>
<th>Administrative</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Characterization</strong></td>
<td>Where is provider's server located?</td>
<td>Who has access to the server?</td>
<td>What is the operating system?</td>
</tr>
<tr>
<td></td>
<td>Is provider's hardware already support trusted computing base?</td>
<td>Does provider has Information Risk Management?</td>
<td>Is it virtualized?</td>
</tr>
<tr>
<td></td>
<td>Is provider's datacenter secured?</td>
<td>Does provider has incident handling procedures?</td>
<td>Is it shared?</td>
</tr>
<tr>
<td></td>
<td>Is provider's rack locked?</td>
<td>What is provider's SLA?</td>
<td>How does provider create</td>
</tr>
</tbody>
</table>
System assessment also must be done at consumer's side to support and work together with provider's assessment system. For example, collecting data about policy documents, current system including web application which will uploaded to provider's system, system design and how they work, procedure, guidelines, security-related documentations, and soon.

### 6.1.2 Threat Identification

Threat means a probability of any party exploiting vulnerabilities exist in the system. Threats has three main components, they are threat sources, vulnerabilities, and existing control to mitigate them. Threat source can be intentional, where system already targeted by sources of threat. Threat source also can be situational, like an accident. Bot threat source intentional or an accident can come from human, natural, and environment. For example, in shared webhosting environment, an attacker can obtain access to another user in same system, and then jump to other user due to lack of protection per user by system, in this case threat source come from natural and system has vulnerabilities to allow another user jump to other users. Usually, threat source from human has motives, therefore company or provider need to assess them and provide necessary protection to mitigate them. Company can use form like table 2 to assess threat identification for outsourcing webhosting:

<table>
<thead>
<tr>
<th>Assessment Point</th>
<th>Threat Source</th>
<th>Likelihood</th>
<th>Threats</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural</td>
<td>Flood, Earthquake, Fire</td>
<td>Fire or flood in datacenter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment</td>
<td>Other tenants, Fiber Optic Overseas, Power Fault</td>
<td>Fiber cut, DDoS unintentional to neighborhood</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 6.1.3 Vulnerability Identification

In this step, company can ask provider about any past vulnerabilities which successfully exploited by threat sources in place for their system and how they handled it. Although this information is sensitive, but with non disclosure agreement between parties, provider can provide this information. Also, company can search in internet related to provider's incidents. Step one which previously collected can be use as another source to identify vulnerabilities. Vulnerability sources information can be identify with table 3 below:
### Assessment Point

<table>
<thead>
<tr>
<th>Vulnerability Identification</th>
<th>Physical</th>
<th>Administrative</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter does not use proper water sprinklers</td>
<td>Previous risk assessment</td>
<td>Security advisories</td>
<td></td>
</tr>
<tr>
<td>Datacenter does not screen people accessing rack/server</td>
<td>IT Security Audit</td>
<td>Vendor advisories</td>
<td></td>
</tr>
<tr>
<td>Rack is not locked</td>
<td>Terminating Employees</td>
<td>Penetration Testing</td>
<td></td>
</tr>
<tr>
<td>Improper cabling</td>
<td>Lack of Patching</td>
<td>Misconfiguration system and network</td>
<td></td>
</tr>
<tr>
<td>Improper power planting</td>
<td>Does not have security policies and standard</td>
<td>Vulnerability database list</td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Vulnerability Identification

As mentioned above that threat without vulnerabilities then there is no risk and vice versa. This connection formulas as:

\[
\text{risk} = \text{threats} \times \text{vulnerability}
\]

and

\[
\text{total risk} = \text{threats} \times \text{vulnerability} \times \text{asset value} \ [13]
\]

In table 4, this illustration can help to understand about relation between threats and vulnerabilities

### Table 4. Relation Threats and Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Threat</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack is not locked</td>
<td>Other tenant access their own rack and has interesting with unlock rack</td>
<td>Other tenant can access company’s rack</td>
</tr>
<tr>
<td>Improper cabling</td>
<td>Mouse</td>
<td>Cable damaged and unplugged</td>
</tr>
</tbody>
</table>

Table 4. Relation Threats and Vulnerabilities

### 6.1.4 Control Analysis

Next step in risk assessment is control analysis. In this step, company can review existing controls which has been implemented or being planned to minimize of probability of threat source against vulnerability. There are 2 categories based on NIST SP800-30 [8], they are preventive and detective.
controls with 2 methods technical and non technical. Furthermore, Shon Harris [13] defines control become 3 types: physical, technical or logical, and administrative control. She is also define 6 categories for control functions: Deterrent, Preventive, Corrective, Recovery, Detective, and Compensating.

<table>
<thead>
<tr>
<th>Categories</th>
<th>NIST SP800-30</th>
<th>Shon Harris</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive</td>
<td>Deterrent</td>
<td></td>
</tr>
<tr>
<td>Detective</td>
<td>Preventive</td>
<td></td>
</tr>
<tr>
<td>Corrective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compensating</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Types</th>
<th>Technical</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non technical</td>
<td>Technical/Logical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrative</td>
<td></td>
</tr>
</tbody>
</table>

Table 5. Control Types and Categories Comparison

Implementation control can use a conceptual Defense-in-Depth. More important or critical company's assets, more control to implement to protect them. For example, company who wants use outsourcing webhosting and provider provide good protection with their system (firewall, IDS/IPS, securing their system, etc) but company can add some controls to their content (for example, encrypt their disk or code before send it to provider's system, add tracker to their document).

6.1.5 Likelihood Determination
Likelihood is a potential vulnerability exercised by a threat with or without existing control to mitigate. The output of likelihood is a rating indicate a possibility chance of exploiting target. Likelihood has 3 components, threat-source motivation or capability, nature of vulnerability (general, specific, easy to launch), and existence of current controls. Below is an example comparison with similar vulnerability but different threat-source:

<table>
<thead>
<tr>
<th>Likelihood Rating</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some ports open to internet</td>
<td>Threat-source has high skill and motivated, some ports has common vulnerabilities and unpatch</td>
<td>Threat-source has high skill and motivated, but most of ports already patched</td>
<td>Threat-source does not have sufficient skill, and all ports open already patched</td>
</tr>
</tbody>
</table>
6.1.6 Impact Analysis
Impact analysis is one of important step. In this step, company will review and analyze the impact if threat source success exercised vulnerability. Company need to collect information about their asset's value, how important them to company, what happen and consequences if threat source success attack vulnerability, and soon. The impact of any incident can be measure with triad CIA (confidential, integrity, and availability). For example, if threat source success attack a vulnerability of an application (buffer overflow) then that application maybe down (loss availability) or data corruption (loss integrity).

In webhosting case, if an attacker success gain access to system with privileged user, then defacing website or stealing data could be happen. Impact analysis can measure with qualitative and quantitative. Quantitative means impact can be count with amount of value (money), qualitative means impact cannot count with amount of value, but described in rating high, medium, and low. Quantitative risk analysis can be formulas as [13]:

\[
SLE = \text{Asset Value} \times \text{Exposure Factor}
\]

where:

- \( SLE \) is single loss expectancy
- \( \text{Exposure Factor} \) is percentage of loss

For example, if a company has 2 servers in a datacenter with each server has value $5000 USD, and one of them stolen (assumes there is not important data, only company profile's website) then:

\[
SLE = (2 \times 5000) \times (50\%) = 5000\ USD
\]

The advantage of quantitative analysis is company can know how much (in money) loss if an incident occurs. But the disadvantages are difficult to value all assets, decrement value, and not all components could be count as money (reputation, human, knowledge, etc).

Qualitative risk analysis is a method which not count components or losses as amount money. For example, in above case if one of server is stolen where company's profile website available then reputation of that company may impact. Therefore, qualitative describe losses as magnitude high, medium, and low.

6.1.7 Risk Determination
Risk determination has purposes to assess risk level by multiplying the likelihood and impact [8]. NIST SP800-30 has an example matrix for risk determination:

6.1.8 Control Recommendations
In this step, risk assessment team provide recommendation controls to implement by company to reduce risk level to an acceptable by company. Some considerations for control recommendations are:
- Existing company policy
- Law and Regulation
- Effectiveness of recommendations
- Operational
Also, those recommendation must aware if recommendation is applicable. Some recommendations may implemented, some of them may not implemented and replace with alternative solutions.

6.1.9 Results Documentation
After risk assessment is done, all results must be documented and report to top management. This document is important for next assessment or if company has significant change. This reports contains about threats, vulnerability, risk measurement, and recommendations control to mitigate or reduce risk.

6.2 RISK MITIGATION
Next process in risk management after risk assessment is risk mitigation. Once top management receive documentation from risk assessment, they can start evaluate and prioritize implementation of risk controls. Selection controls must reduce risk to an acceptable level with least cost approach [8]. Risk mitigation has 4 components: Risk Mitigation Options, Strategy, Control Implementation, and Control Categories.

6.2.1 Risk Mitigation Options
NIST SP800-30 defines 6 options for risk mitigation [8], they are:
- Risk Assumption or Acceptance means accept current or potential risk and continue activity. Or implement approved controls to reduce risk to an acceptable level.
- Risk Avoidance, avoid potential risk and discontinue activity since there is no sufficient control to reduce it to an acceptable level.
- Risk Limitation, limiting risk by implement control with minimum impact to business
- Risk Planning, manage control selections and implementation control including monitoring and maintains controls
- Research and Acknowledgment, reduce risk by research and acknowledgment of vulnerability and implement control to remove or correcting vulnerability
- Risk Transference, transferring risk to other party for compensating of loss risk. An example is purchasing insurance.
Company must identified and prioritize risk from highest to lower risk. It is near impossible to identified all risk in company, so the key is prioritize and applicable.

6.2.2 Risk Mitigation Strategy
Strategy is one of important things in risk mitigation. Some questions may rise up at top management while thinking or decide what to do with risk assessment report, what things should they must do or what is prioritize. One way is to creating pair of threat/vulnerability. From formula above about risk, if there is no vulnerability, but threat source already identified, then there is no need mitigate them because risk is zero. Hence, top management can start with pairing threat source and vulnerability and then prioritize them from highest impact to lowest impact.

6.2.3 Control Implementation
Next is control implementation. It is useless if company already done with risk assessment, approved control selection, define strategy to implement them, but still they did not take any action to implement to real world. So this step is about implementation and must follow de facto rules: "Define what is the highest risk and then select control to reduce it to an acceptable level of risk with lowest cost". There are some steps already define by [8]:
- Prioritize Actions, sort any risk from highest to lowest
- Evaluate Control which is proposed, controls must be effective and applicable.
- Cost/Benefit Analysis, selected control from previous step must be compare with cost/benefit gains after implementation. For example, it is overkill if a company decide put their company's profile website without important data to dedicated server which cost around hundreds thousands dollar a month.
- Select Control, After do some analysis with cost/benefit above, top management must define which control must be implemented.
- Assign Responsibility, management can assign who will implement selected controls, who will supervise, and who will validate implementation.
- Developing a Safeguard Implementation Plan, Company must create plan during implementation safeguard, from selected control which already define before. This plan is like project management which contains about: threat, vulnerability, risks level, recommended controls, prioritize, selected control, resources, list of assigned personal to implement, detail of date time, target of implementation, and maintains of safeguard.
- Implement selected controls, after implementation some risks may successfully reduced to lower level, but not completely eliminate them. This risks called residual risk with formula:

$$\text{total risk} - \text{countermeasure (or safeguard)} = \text{residual risk} \quad [13]$$

### 6.2.4 Control Categories
As discuss above (6.1.4), control has 2 main categories [8] but [13] define them as 3 main categories with additional category is physical (administrative can be assume as non technical). The most important for control categories is about how company define and implement control in the right place to mitigate risks.

### 7. CONCLUSION
Outsourcing webhosting still one of the best option for company who does not have sufficient resources to manage it. But company need to assess risk through risk management to mitigate any risks which may arise from outsourcing webhosting. Company and provider must work together, honest and diligent to achieve requirements for both parties. For company, they can use webhosting with minimum cost and risk, and focus with their business. For provider, this can be good practice for providing secure outsourcing webhosting which already define (and could be validate with some standard) and making new opportunity for next client. NIST SP800-30 is one of standard for risk management guide for information technology systems. Although this standard focused on IT and computer systems security without cover about business risk (or relation between security risks to business risk) but it is already good enough for purpose of this paper.

### REFERENCES


