HELIXSTORM

NETWORK ASSESSMENT

IT SWOT Analysis

Prepared by: Helixstorm
Prepared for: Sample Company 6/1/2013

ABOUT THIS REPORT

The IT SWOT analysis is a structured method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats affecting an IT network. The analysis involves identifying internal and external issues that are favorable and unfavorable to increasing the overall network health and security of the environment. After the SWOT analysis has been performed, a list of recommendations and suggestions will be developed based upon achievable goals and objectives of the organization.

Strengths and Weaknesses are internal to the organization and include issues the organization has direct control over. For example, deciding whether to replace old computer hardware, moving to a hosted mail service, allowing mobile device use or upgrading to a new operating system. Opportunities and Threats are external to the organization and therefore cannot be controlled directly. For example, evaluating carrier bandwidth, identifying security issues associated with wireless communications, recognizing risks of being located in geographically unstable areas prone to earthquake or hurricane.

Identification of SWOTs is important because they form the basis in planning to achieve realistic IT objectives.

ISSUES SUMMARY

SWOT	Helpful …to achieving the objective	Harmful …to achieving the objective
Internal Origin (Attributes of the organization)	***STRENGTHS***	***WEAKNESSES***
	1. WPA2 security for wireless access is considered acceptable. (KP0) 2. Devices are well-labeled in the server room. (KP1)	1. Lack of monitor could cause unnecessary productivity loss. (KP2) 2. Lack of mobile device policy can lead to liability and other legal concerns. (KP3) 3. Lack of humidity control could lead to moisture problems in server room. (KP4) 4. Employees are spending time skipping spam messages due to lack of spam filtering. (KP5)
External Origin (Attributes of the environment)	***OPPORTUNITIES***	***THREATS***
	1. Newer available VoIP technology could increase functionality and cost savings. (KP6) 2. Ink management service could provide extreme value and cost savings. (KP7) 3. MDM of BYOD devices will mitigate legal and management concerns. (KP8) 4. Cable management could easily be implemented to improve appearance and prevent outage causing mistakes. (KP9) 5. Hardware refresh of workstations would lead to faster performance and productivity gains. (KP10)	1. Without MDM, viruses, spyware, and malicious apps could compromise sensitive data and LOB apps. (KP11) 2. Allowing users to install their own remote access methods invites multiple points of entries for hackers. (KP12) 3. Lack of UPS or redundant power in the server room could lead to a major outage. (KP13) 4. End of life for Windows XP on the horizon. Lack of updates could lead to security issues. (KP14) 5. Unfiltered spam could lead to fishing messages making it through and causing harm to individual computers as well as the network. (KP15) 6. No recovery from catastrophic disaster due to lack of offsite backup. (KP16)

HARDWARE

Weaknesses:

- ☑ Lack of monitor could cause unnecessary productivity loss. (KP2)

Opportunities:

- ☑ Newer available VoIP technology could increase functionality and cost savings. (KP6)
- ☑ Ink management service could provide extreme value and cost savings. (KP7)

MOBILE COMPUTING

Strengths:

- ☑ BYOD shifts the cost of devices to the employee
- ☑ WPA2 security for wireless access is considered acceptable. (KP0)

Weaknesses:

- ☑ Lack of mobile device policy can lead to liability and other legal concerns. (KP3)
- ☑ Lack of centralized management of remote access could invite a breach.

Opportunities:

- ☑ MDM of BYOD devices will mitigate legal and management concerns. (KP8)

Threats:

- ☑ Without MDM, viruses, spyware, and malicious apps could compromised sensitive data and LOB apps. (KP11)
- ☑ Allowing users to install their own remote access methods invites multiple points of entries for hackers. (KP12)

+0*20* *''4

Strengths:

- ☑ Essential servers are stored in a centralized location.
- ☑ Devices are well-labeled in the server room. (KP1)
- ☑ Dedicated server room climate control.

Weaknesses:

- ☑ Sever equipment is randomly located in the rack causing various layout and management problems.
- ☑ Cabling is interwoven and random.
- ☑ Lack of humidity control could lead to moisture problems in server room. (KP4)

Opportunities:

- ☑ Cable management could easily be implemented to improve appearance and prevent outage causing mistakes. (KP9)

Threats:

- ☑ Lack of UPS or redundant power in the server room could lead to a major outage. (KP13)

WORKSTATIONS

Strengths:

☑ Individual UPS are attached to every workstation.

Opportunities:

☑ Hardware refresh of workstations would lead to faster performance and productivity gains. (KP10)

Threats:

☑ End of life for Windows XP on the horizon. Lack of updates could lead to security issues. (KP14)

CURRENT SERVICE

Strengths:

- ☑ Onsite backup is employed and centrally managed.

Weaknesses:

- ☑ Employees are spending time skipping spam messages due to lack of spam filtering. (KP5)

Opportunities:

- ☑ Spam filter is available inexpensively and can be implemented without moving providers.
- ☑ Migration to Office 364 could combine all email accounts company- wide and allow for centralized management.

Threats:

- ☑ Unfiltered spam could lead to fishing messages making it through and causing harm to individual computers as well as the network. (KP15)
- ☑ No recovery from catastrophic disaster due to lack of offsite backup. (KP16)