HELIXSTORM

NETWORK ASSESSMENT

# QUARTERLY BUSINESS REVIEW

**Prepared by:** Helixstorm
**Prepared for:** Prospect Or Customer 10/29/2014

## TABLE OF CONTENTS

# I - INTRODUCTION

Understanding business requirements and aligning them with the correct Information Technology plans is critical to getting the best return on your investment. This is true whether the objective is to enhance productivity, meet regulatory compliance or just to maintain current systems and achieve lower cost of ownership.

We do not believe technology should drive your decisions. Rather, our approach to IT initiatives for your business is to focus on aligning business needs with IT. We believe the business need once identified, will drive the IT process. Through our consultative approach, IT goals and initiatives become apparent and form the basis for your IT road map.

With our combined technology and business focus, we will help you identify the right technology solutions that can deliver high value while controlling costs. We also want to ensure that we are meeting our commitments to your organization and scheduling future services to conform to agreed objectives.

On a quarterly basis your plan is reviewed and updated, as necessary, to address new business situations. We also provide an analysis of current system health and go over the status of any open projects. Your staff and our team examine IT items in detail, one by one. Projects timelines and budgets are discussed; audit and compliance issues are addressed as well as service level items. Follow up action items are then defined and delegated.

The Quarterly Business Review helps make sure that your IT business objectives are managed more effectively and expectations properly set.

# 2 - PREVIOUS QUARTER PERFORMANCE REVIEW

In this section, we will review key metrics and significant changes to the network.

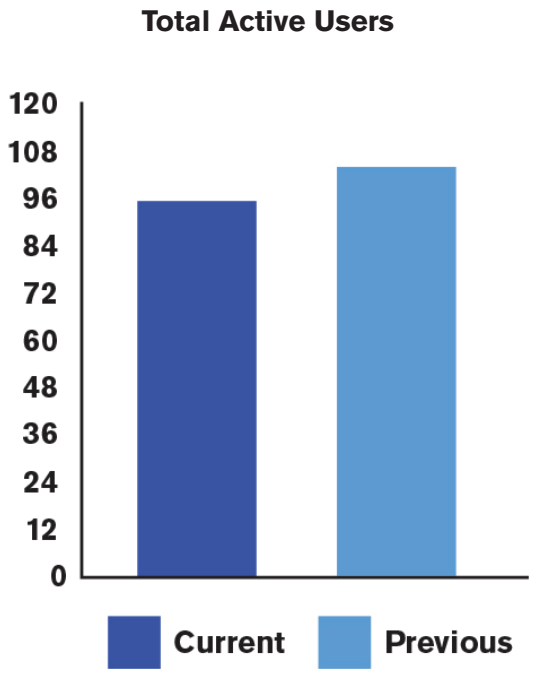
## 2.1 - KEY METRICS

| | Current | Previous | Trend |
|---|---|---|---|
| **Total Active Computers** | 44 | 51 | -7 |
| **Total Active Users** | 16 | 17 | -1 |
| **Total Active Anti-virus Coverage** | 34.09% | 39.22% | -5.13% |
| **Backup Coverage** | 9.09% | 7.84% | +1.25% |
| **Patch Coverage** | 70.45% | 80.39% | -9.94% |

## 2.2 - DOCUMENTATION OF CHANGES

### Computers

During the previous quarter *0 computer(s) were added, and 9 computer(s) were removed.*



| Action | Type | Detail |
|---|---|---|
| **REMOVED** | Windows 7 Enterprise | DIMAGIO-SG |
| **REMOVED** | Windows 7 Enterprise | DELL120720 |
| **REMOVED** | Windows XP Professional | HJOBS-VM-WIN764 |
| **REMOVED** | Windows 7 Enterprise | LEE |
| **REMOVED** | Windows 7 Enterprise | NETSCAN01 |
| **REMOVED** | Windows 7 Enterprise | PERSHING-MYCO |
| **REMOVED** | Windows 7 Enterprise | PSANDOVAL-WIN764 |
| **REMOVED** | Windows 7 Enterprise | USAL9K49RH1 |

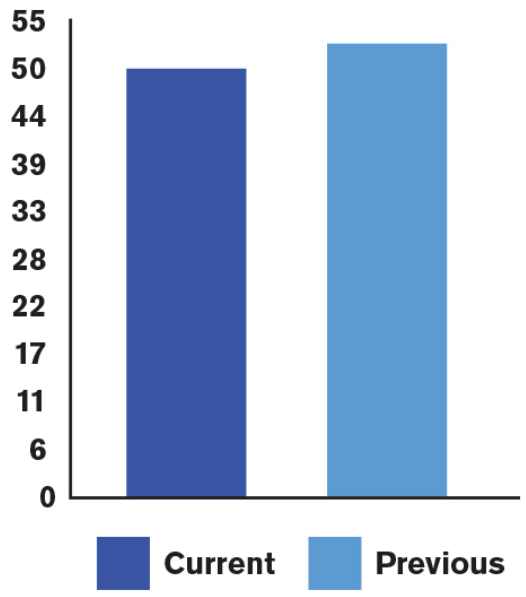
## Printers

*No printer changes occurred during the quarter*

## Users and Access

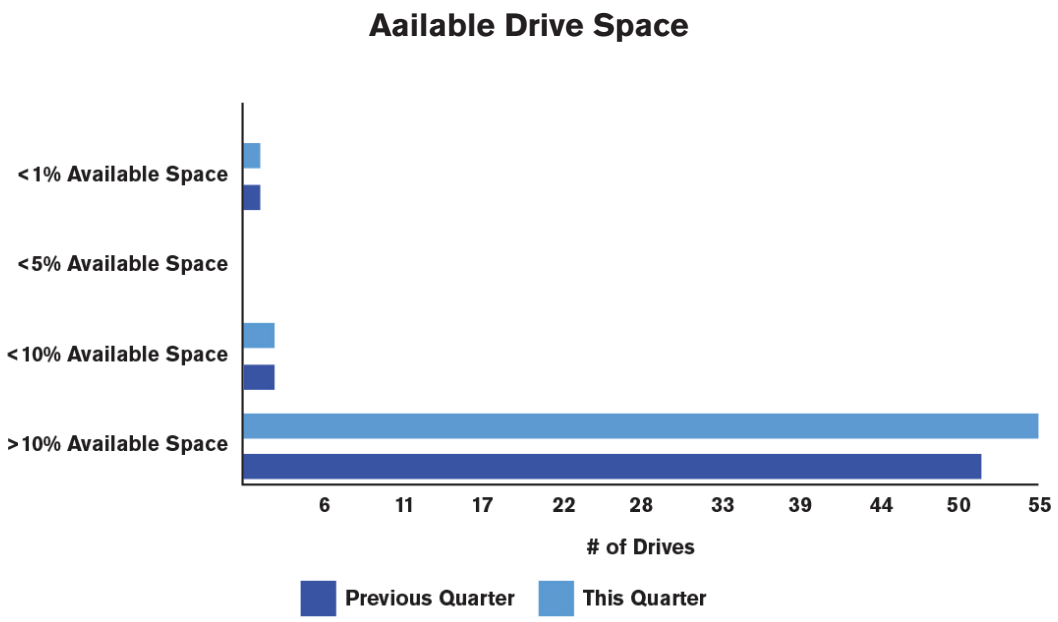
During the previous quarter*1 user(s) were added, 0 user(s) were disabled, and 4 user account(s) were deleted. Also, 8 change(s) in security group (access) occurred.*

**Total Active Users**



| Action | Type | Detail |
|---|---|---|
| ADDED | User | Jennifer Smith |
| MODIFIED | Security Group | Administrators(Removed: Henry Jobs) |
| MODIFIED | Security Group | AppV Administrators(Added: Jennifer Smith)(Removed: Joe DiMagio) |
| MODIFIED | Security Group | AppV Administrators(Added: Jennifer Smith)(Removed: Joe DiMagio) |
| MODIFIED | Security Group | DHCP Administrators(Removed: Henry Jobs) |
| MODIFIED | Security Group | Domain Admins(Added: Jennifer Smith)(Removed: Henry Jobs,Joe DiMagio,Dave Bartlett) |
| MODIFIED | Security Group | Enterprise Admins(Removed: Dave Bartlett) |
| MODIFIED | Security Group | MYCO Support Team(Added: Jennifer Smith)(Removed: Henry Jobs,Joe DiMagio,Dave Bartlett) |
| MODIFIED | Security Group | Schema Admins(Removed: Dave Bartlett) |
| DELETED | User | Dave Bartlett |
| DELETED | User | Henry Jobs |
| DELETED | User | Joe DiMagio |
| DELETED | User | Net Scanner - PerformanceIT |

## Storage



| Computer | Drive | Space Available |
|---|---|---|
| MAINPATCH | C: | 2.74 GB |
| PSANDOVAL1 | C: | 4.82 GB |
| MODIFIED | C: | 0 GB |

## External Speed Analysis

Please note that the external speed analysis is a point in time analysis and should only be used as a reference.

| Computer | Min | Max |
|---|---|---|
| This Quarter | 1.85 Mb/s (Tokyo, Japan) ↑ | 4.03 Mb/s (Atlanta, Georgia) ↓ |
| Previous Quarter | 0.06 Mb/s (Amsterdam, The Netherlands) | 4.15 Mb/s (Chicago, Illinois) |

# 3 - ISSUES REVIEW

## 3.1 - ADDRESSED ISSUES

### Inactive Users
***Previous Issue:*** We discovered 23 active user accounts that have not logged in within the past 30 days.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Inactive Computers
***Previous Issue:*** 53 computers were found as having not checked in during the past 30 days.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Organizational Units
***Previous Issue:*** We discovered 0 populated Organizational Units.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Domain Controllers
***Previous Issue:*** 2 offline domain controllers were discovered and should be investigated. An offline domain controller may be a remnant of decommissioning a server which was not properly removed from the domain. With 0 online Domain Controllers, there is a heightened risk of business downtime, loss of data, or service outage due to a lack of redundancy.
***Status:*** *No longer an issue*

### Password Strength Risks
***Previous Issue:*** Local Account Passwords on 1 computer were found to have a Potential Risk. 10 computers were found to have a Severe Risk. These are systems where passwords are extremely weak or are not required.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Password Policies
***Previous Issue:*** Issue: 29 enabled domain users have passwords that are set to never expire.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Insecure Listening Ports
***Previous Issue:*** 7 computers were found to be using potentially insecure protocols.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Operating System Support
***Previous Issue:*** 40 computers were found to be using an Operating System that is in Extended Support. 6 computers were found to be using an Operating System that is no longer supported by the manufacturer and should be upgraded.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Critical Patches Missing

***Previous Issue:*** 10 computers were detected as having 1 or more missing critical patches.
***Status:*** *Still an issue but improved. See Current Issues list.*

### Endpoint Security

***Previous Issue:*** Anti-virus and anti-spyware was scanned for but not detected on 31 computers.
***Status:*** *Still an issue but improved. See Current Issues list.*

## 3.2 - CURRENT ISSUES

### Inactive Users

***Issue:*** We discovered 21 active user accounts that have not logged in within the past 30 days.
***Recommendation:*** Active accounts that are not in use may pose an inherent security risk, especially those that have been used for a prolonged period of time and should be addressed with a User Audit. These accounts should be reviewed and disabled or removed if they are no longer needed. The accounts could be used by a malicious attacker both internally and externally. The National Institute of Standards (NIST) recommends disabling any account with 90 days of inactivity. We suggest reviewing active users and disabling or removing accounts which are no longer needed.

### Inactive Computers

***Issue:*** 51 computers were found as having not checked in during the past 30 days.
***Recommendation:*** By itself, this does not pose a serious threat, but proper organization and management is essential for good network administration and to providing accurate domain statistics and information. Inactive computers in active directory may represent computers that are no longer in use. While this poses limited risk to the organization, we recommend a more detailed and thorough review of Active Directory to identify machines that have not reported in and removing all defunct entries.

### Organizational Units

***Issue:*** We discovered 0 populated Organizational Units.
***Recommendation:*** It's a good idea to periodically review the details of the Organization Units to ensure they align with your business and operational needs. Proper alignment is crucial to ensuring security and access policies are adhered to properly. Organization Units (OU) are the building blocks of good network security in an Active Directory environment. While there is no correct answer to the proper number of OUs required, having too few is an indicator that the OU structure may not be in line with the security needs of the company. We suggest reviewing the business organizational structureand security needs to ensure the proper Organizational Units (OU) structure is in place.

### Password Strength Risks

***Issue:*** Local Account Passwords on 2 computers were found to have a Potential Risk. 14 computers were found to have a Severe Risk. These are systems where passwords are extremely weak or are not required.
***Recommendation:*** Inadequate or weak passwords on local accounts can allow a hacker to compromise the system. It can also lead to the spread of malicious software that can cause business and productivity affecting issues. We recommend placing adequate password strength requirements in place and remediate the immediate password issues on the identified systems.

### Password Policies

***Issue:*** Issue: 25 enabled domain users have passwords that are set to never expire.
***Recommendation:*** The best practice for passwords is to change them on a routine basis. While convenient (and in the case of Service Accounts appropriate), account passwords that are set to never expire pose a significant security risk. We advise identifying if the accounts listed have a legitimate need for having the password never expire (as in the case of Service Accounts) or should have its policies modified.

### Insecure Listening Ports

***Issue:*** 22 computers were found to be using potentially insecure protocols.
***Recommendation:*** There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they typically lack encryption. Inside the network, their use should be mineralized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security.

### Operating System Support

***Issue:*** 38 computers were found to be using an Operating System that is in Extended Support. 6 computers were found to be using an Operating System that is no longer supported by the manufacturer and should be upgraded.
***Recommendation:*** Extended Support means patching and other updates will be unavailable in the near future. Operating system versions that are no longer supported pose a significant security risk as security holes will no longer be addressed. OSes in Extended Support are nearing end of life and should be upgraded before the end of life. We propose reviewing the function and criticality of computers in Extended Support and upgrading systems that are no longer supported.

### Critical Patches Missing

***Issue:*** 13 computers were detected as having 1 or more missing critical patches.
***Recommendation:*** Maintaining properly patched systems reduces the risk of infection via malware or viruses and improves performance and stability. Unpatched systems are also less protected against malicious software attacks. This can pose a significant risk to your network. We strongly recommend applying missing patches on identified computers immediately.

### Endpoint Security

***Issue:*** Anti-virus and anti-spyware was scanned for but not detected on 29 computers.
***Recommendation:*** Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant. Since this can lead to both security and productivity issues, we strongly recommend assuring anti-virus and anti-spyware are deployed to all possible endpoints.

# 4 - SWOT ANALYSIS

We've conducted a review of your current strengths, weaknesses, opportunities and potential threats. Understanding both your strengths and weaknesses can help us formulate an action plan that will allow us to improve the reliability and performance of your network.

## 4.1 - STRENGTHS

These are the strengths we identified in your business. These are both administrative and technical assets you have that you can build on.

- No strengths were identified

## 4.2 - WEAKNESSES

Weaknesses are areas where we have identified room for improvement.

- No weaknesses were identified

## 4.3 - OPPORTUNITIES

These are potentials for improvements in your environment. By leveraging opportunities, we can help you improve your infrastructure.

- No opportunities were identified

## 4.4 - THREATS

Threats are external dangers to your IT infrastructure. Some dangers are more immediate than others.

- No threats were identified

## 5 - ACTION PLAN

We propose the following action plan to address your current weaknesses and threats.

### INSERT YOUR PROPOSED ACTION PLAN